STRATECON
TECH ADVISORS

ARTIFICIAL INTELLIGENCE USE POLICY (AIUP)

TEMPLATE

WWW.STRATECON.TECH

About this Template

Creating an AI Use Policy (AIUP) for a company is a complex task that requires input from various stakeholders. The policy should address all the key areas of concern that could create privacy, security, or legal issues. The policy should also be flexible enough to accommodate future changes in technology and regulations. It's important to note that creating an AI policy is not a one-time event. It should be reviewed and updated regularly to ensure that it remains relevant and effective.

The below template is provided for informational purposes only and is designed as a starting point to help organizations craft their own customized AI Use Policy. There may be additional areas that individual organizations will wish to consider in their AIUP. Organizations should consult with their trusted cybersecurity and legal experts to build their final AIUP document. If you would like assistance in that process, Stratecon Tech Advisors is available to help. Please reach out to us to schedule a conversation – info@stratecon.tech.

Company Artificial Intelligence Use Policy (AIUP)

Introduction

This AI policy is designed to establish clear guidelines for the acceptable and responsible use of artificial intelligence (AI) technologies within our company. It is a collaborative effort between our cybersecurity professionals and corporate lawyers to address the key areas of concern that could potentially create privacy, security, or legal issues.

1. AI Development and Deployment

a) **Transparency and Accountability:** All AI projects must be transparent in their objectives, methodologies, and potential impacts. An accountable team should oversee each AI project, with a designated person responsible for ensuring compliance with this policy. The accountable team member should document how AI decisions are made and how they can be explained to stakeholders.

b) **Ethical Considerations:** The company shall use AI in a manner that is ethically sound, respects human rights, and avoids any form of discrimination. AI systems shall not be used to perpetuate biases, and steps must be taken to mitigate bias in training data.

c) **Data Privacy:** AI projects shall adhere to all relevant data protection regulations (e.g., GDPR, CCPA). Data used for AI training and inference must be collected, processed, and stored securely, with explicit user consent whenever necessary.

2. Security

a) **Risk Assessment:** Before deploying AI solutions, a comprehensive security risk assessment must be conducted. This assessment should identify potential vulnerabilities, threats, and countermeasures. This includes reviewing the tool's security features, terms of service, and privacy policy. Employees must also check the reputation of the tool developer and any third-party services used by the tool.

b) **AI Disclosure Statements:** For each AI tool utilized within the company, an AI Disclosure Statement should be completed and kept up to date. The Disclosure Statement should document the information being captured by AI models, where and how it is stored, how it is used, how AI features can be enabled/disabled, and which parties own the information generated by AI. If any information is being shared with third parties because of utilizing AI features, AI Disclosure information for those third parties should also be gathered.

c) **Data Security:** AI models and associated data must be protected against unauthorized access, both internally and externally. Encryption, access controls, and regular security audits should be employed.

d) **Protection of confidential company data:** Employees must not upload or share any data that is confidential, proprietary, or protected by regulation without prior approval from the appropriate department. This includes data related to customers, employees, or partners.

e) **Access control:** Employees must not give access to AI tools outside the company without prior approval from the appropriate department or manager and subsequent processes as required to meet security compliance requirements. This includes sharing login credentials or other sensitive information with third parties.

f) **Use of reputable AI tools:** Employees should use only reputable AI tools and be cautious when using tools developed by individuals or companies without established reputations. Any AI tool used by employees must meet our security and data protection standards.

g) **Compliance with security policies:** Employees must apply the same security best practices we use for all company and customer data. This includes using strong passwords, keeping software up-to-date, and following our data retention and disposal policies.

h) **Incident Response:** An AI-specific incident response plan must be developed, detailing the steps to be taken in case of a security breach related to AI systems. Employees should be trained on this plan.

3. Legal Compliance

a) **Intellectual Property:** Intellectual property rights related to AI development should be clearly defined. Ownership of AI models, algorithms, and associated patents must be established according to company policies. If AI models are generating content, it should be clearly documented who owns that content, and what are the acceptable uses of said content.

b) **Liability and Accountability:** The company shall define clear lines of liability and accountability for the actions and decisions made by AI systems. Human oversight must be maintained where necessary, especially in critical decision-making processes.

c) **Regulatory Compliance:** AI projects must comply with relevant industry-specific regulations. Regular legal reviews should be conducted to ensure ongoing compliance.

4. Employee Training and Awareness

a) **Education:** Employees involved in AI projects should receive regular training on the ethical, legal, and security aspects of AI. This includes understanding the potential impacts of AI on privacy and the importance of data protection.

b) **Reporting:** Employees should be encouraged to report any AI-related concerns, security vulnerabilities, or potential legal issues through a designated channel. Whistleblower protection must be provided.

5. Ongoing Review and Improvement

This AI policy shall be periodically reviewed and updated to reflect changes in technology, regulations, and company practices. Feedback from cybersecurity professionals, corporate lawyers, and relevant stakeholders shall be considered to ensure the policy's effectiveness and relevance.

6. Conclusion

By adhering to this comprehensive AI policy, we aim to harness the potential of AI while maintaining the highest standards of privacy, security, and legal compliance within our company. Our organization is committed to ensuring that the use of AI tools is safe and secure for all employees and customers, as well as the organization itself. We believe that by following the guidelines outlined in this policy, we can maximize the benefits of AI tools while minimizing the potential risks associated with their use.

7. Acknowledgement and Compliance

All employees must read and sign this policy before using any AI tools in the organization. Failure to comply with this policy may result in disciplinary action, up to and including termination.

By signing this policy, I acknowledge that I have read and understand the requirements outlined in this policy. I agree to use AI tools in a manner consistent with the security best practices outlined above and to report any security incidents or concerns to the appropriate department or manager.

Employee Signature: _____

Date: _____