ROCHESTER BUSINESS JOURNAL
Part of the BRIDGETOWER MEDIA network
FEBRUARY 15, 2024

Crafting an effective AI acceptable use policy

AI Demystified

By Richard Marinaccio & Dorothy Shuldman, Phillips Lytle LLP

Richard Marinaccio

Dorothy Shuldman

As artificial intelligence (AI) technologies continue to increase in popularity and demand across industries, so does the need for robust governance frameworks to guide their ethical and responsible use. Recognizing this imperative, organizations can turn to established frameworks to inform the development of comprehensive AI acceptable use policies. Among these frameworks, the National Institute of Standards and Technology's (NIST) AI Risk Management Framework (AI RMF) offers a structured approach that aligns with best practices and regulatory requirements. The AI RMF is a non-sector-specific voluntary resource for organizations to use when developing, implementing or using AI systems to manage AI risks and promote trustworthy and responsible AI use. In this article, we will explore how businesses can leverage the NIST framework to draft and implement AI acceptable use policies that foster trust, transparency and accountability.

UNDERSTANDING THE NIST FRAMEWORK

The NIST's AI RMF is designed to help organizations address the challenges of AI deployment by promoting trust, transparency and accountability throughout the AI lifecycle. According to NIST, trustworthy AI systems are: valid and reliable, safe, secure and resilient, accountable and transparent, explainable and interpretable, privacy-enhanced, and fair.

The NIST created the AI RMF playbook with suggested procedures for organizations to follow to achieve their goals. The AI RMF consists of the four functions below:

1. *Govern:* Addresses the overarching policies, procedures and controls governing AI usage to support compliance with legal, ethical and regulatory requirements.
2. *Map:* Recognizes the context, risk and impact of AI use. This phase also identifies the processes and practices involved in AI system development, deployment and maintenance.
3. *Measure:* Metrics are established, and risks are assessed, analyzed or tracked.
4. *Manage:* Involves the ongoing assessment and validation of AI systems' risks, performance, reliability and adherence to policy guidelines.

AI ACCEPTABLE USE POLICIES

Drafting an AI acceptable use policy is an important first step for an organization to take to effectively outline the guidelines, rules and procedures governing the development, deployment and utilization of the AI systems in use or planned for future use, and to align such policy with their organization's risk tolerance. Internal AI policies can serve as a roadmap for employees, outlining permissible use cases, data handling practices, transparency requirements and accountability measures concerning AI technologies. As AI's applicability rapidly expands across industries, it is recommended that organizations take the steps to understand their goals and risk tolerance when implementing and using AI, and to draft and implement the policy in a manner that aligns their workforce's practices with their goals and values.

RECOMMENDATIONS FOR DRAFTING AI ACCEPTABLE USE POLICIES

Depending on the industry, nature and complexity of your organization, some or all of the following should be considered when working on your AI policies:

1. *Conduct a comprehensive risk assessment:* Before drafting the policy, conduct a thorough risk assessment to identify potential risks associated with AI deployment. These risks may include data privacy breaches, algorithmic bias, security vulnerabilities, regulatory non-compliance, and ethical considerations. By understanding these risks upfront, organizations can develop mitigation strategies and incorporate relevant safeguards into the policy framework.
2. *Define clear objectives and scope:* Begin by clearly defining the objectives and scope of the AI acceptable use policy. Identify the specific AI technologies covered, such as machine learning algorithms, natural language processing systems or robotic process automation. Then, articulate the intended purposes and limitations of their usage within the organization. An organization should also identify specific third-party solutions that may be governed by contract, as contractual obligations should be considered in the creation of the policy.
3. *Ethical principles and bias mitigation:* Embed ethical principles and values into the policy framework to help AI applications better align with organizational values and promote trust. Consider principles such as fairness, transparency, accountability and privacy when formulating guidelines for AI development and deployment. Implement measures to identify and mitigate biases in AI algorithms. Encourage diverse and representative data collection practices, conduct bias assessments regularly and incorporate fairness-aware techniques during algorithm development to minimize the risk of discriminatory or unjust outcomes.
4. *Data governance, privacy and incident response:* Establish robust data governance and privacy guidelines to govern the collection, storage, processing and sharing of data used by AI systems. Evaluate compliance with relevant data protection regulations — for example, the European Union's General Data Protection Regulation (GDPR), New York's Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) or the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA) — and incorporate measures to protect sensitive information, uphold individual privacy rights and establish procedures in the event of a breach.
5. *Transparency and explainability:* Promote transparency and explainability in AI systems by requiring developers to document the decision-making processes, algorithms and data sources used in AI models. Encourage the use of interpretable and understandable AI models, especially in applications involving sensitive healthcare or financial data, where transparency is paramount.
6. *Accountability and oversight:* Establish clear lines of accountability and oversight for AI development, deployment and monitoring. Designate responsible individuals or establish task forces for overseeing AI projects, conducting audits, and addressing issues related to compliance, ethics and risk management.
7. *Continuous evaluation and improvement:* Regularly review and update the AI acceptable use policy to adapt to evolving technological advancements, regulatory changes and organizational needs. Request feedback from employees and other stakeholders (for example, customers), monitor compliance with policy guidelines, and incorporate lessons learned from past experiences to enhance the effectiveness and relevance of the policy framework over time.

BEST PRACTICES FOR IMPLEMENTATION OF AN AI ACCEPTABLE USE POLICY

While this is not a one-size-fits-all approach and will depend on the structure of your organization, some or all of the following should be considered after the policy is drafted and you are ready for implementation:

1. *Top-down leadership support:* Secure buy-in and support from senior leadership, which will support the successful implementation and enforcement of AI acceptable use policies across the organization.
2. *Multidisciplinary approach:* Implementing an AI acceptable use policy involves collaboration across various departments, including but not limited to legal, compliance, IT, data science and business units. Forming a cross-functional task force or team with representatives from these areas allows for the consideration of diverse perspectives and the organization's collective goals and priorities.
3. *User-friendly documentation:* Create user-friendly and easily accessible documentation that clearly communicates policy guidelines, procedures and expectations to all relevant stakeholders, including employees, contractors and third-party vendors.
4. *Regular training and communication:* Conduct regular training sessions, workshops and communication initiatives to keep employees informed about AI policies, updates, best practices and risks in the event of violations of the policy. Raise awareness among employees about the importance of AI ethics and compliance through training programs, workshops and communication initiatives. Provide employees with the knowledge and tools they need to adhere to the policy guidelines and recognize the risks in AI usage.
5. *Monitoring and enforcement procedures:* Establish robust monitoring and enforcement mechanisms to facilitate compliance with the AI acceptable use policy. Implement regular audits and assessments to monitor AI systems' performance, adherence to policy guidelines and alignment with regulatory and ethical standards. Specify consequences for policy violations and establish channels for reporting concerns or ethical issues related to AI usage.
6. *Adapt based on feedback:* AI technologies and regulatory landscapes are constantly evolving, requiring organizations to adapt their policies accordingly. Solicit feedback from employees and stakeholders, monitor emerging trends and developments in AI governance, and be prepared to update the policy periodically to reflect new insights, best practices and regulatory changes. Continuous oversight and improvement is key to maintaining the relevance and effectiveness of the AI acceptable use policy over time.
7. *Comprehensive risk management:* Implement robust risk management processes to identify, assess, and mitigate risks associated with AI deployment, including technical failures, security breaches, ethical lapses and legal liabilities.

Leveraging the NIST's AI RMF provides organizations with a structured approach to drafting AI acceptable use policies that promote trust, transparency and accountability in AI deployment. As AI technologies continue to evolve, organizations must remain vigilant in adapting their policies to address emerging challenges and regulatory requirements. By addressing key components such as data governance, model transparency, development processes, compliance and evaluation, businesses can develop policies that mitigate risks and foster responsible AI stewardship. Organizations that embrace a proactive approach to AI governance will not only enhance efficiency and confidence in AI systems, but allow AI to remain a force for positive change for their business.

Richard J. Marinaccio is a partner at Phillips Lytle LLP and leader of the firm's Artificial Intelligence Team. He can be reached at rmarinaccio@phillipslytle.com or (716) 504-5760.

Dorothy E. Shuldman is an attorney at Phillips Lytle LLP and a member of the firm's Corporate and Business Law Practice and Intellectual Property Team, focusing on trademark and copyright law. She can be reached at dshuldman@phillipslytle.com or (716) 504-5778.