



Artificial Intelligence Policies

They create a blueprint for success

by: Christina Catenacci & Tommy Cooke, voyAIge strategy Inc.

Artificial intelligence (AI) is at the forefront of innovation and opportunity. In fact, it is projected that AI will have an estimated 21% net increase on the United States' GDP by 2030. For technology vendors, this presents both a massive opportunity and a significant risk.

To thrive in this new AI-driven economy, businesses need more than just powerful algorithms — they need clear plans. AI policies are the blueprints that ensure AI is leveraged effectively, securely and profitably. Think of AI policies as playing both offense and defense for your company: they drive growth and innovation while protecting the company from legal, reputational and operational risks.

AI policies are about much more than managing risk. They give companies a competitive edge. For example, imagine two competing software sales companies: Company A allows employees to use AI freely without guidelines or restrictions. Sales teams are using AI to draft client emails, generate customer insights and analyze market data. But without clear AI policies in place, sensitive customer data is sometimes exposed and AI-generated sales reports are often misleading.

Company B has a defined AI policy that outlines how AI can be used in sales, including guidelines on data privacy, customer interaction and report generation. Sales teams not only have clear instructions on how to and how not to use AI, but they are working in lockstep — everyone is performing within the rules, creating efficient, consistent workflows that leaders trust will work.

Which company would you trust to handle your business data and provide accurate sales insights? Clear AI policies allow businesses to align AI use with business goals, improve customer confidence and avoid disruptions. They give companies a tactical advantage, allowing them to innovate while maintaining control.

AI can also introduce complex risks, such as data privacy breaches, copyright violations, algorithmic bias and reputational damage. Without clear guidelines, minor mistakes can lead to major financial and legal consequences. This means that AI policies serve as a defensive shield by establishing clear rules and expectations for how AI is used across the organization. They define what is and is not an acceptable use.

For instance, let's consider an HR manager who is drafting an AI policy to prevent copyright infringement in AI-generated content. By defining AI inputs, setting content review standards and explaining consequences, the company can avoid legal action while encouraging the creative use of AI.

Another defensive feature of AI policies is that they generate



alignment with the law. Certain states currently have their own comprehensive AI laws; for example, California, Utah, Colorado and Virginia have led the way. Also, many states have data privacy laws that relate to how AI can be used. AI policies aligned with evolving legal requirements ensure compliance, reduce liability and position the company to adapt quickly to new regulations, turning legal alignment into a competitive edge.

AI policies do not slow down business — they empower companies to innovate within a safe, trust-building framework. When employees understand the rules, they make smarter decisions because they have confidence in knowing what is expected of them and they know what not to do.

Many companies try to take shortcuts with AI policies by buying, copying and scraping together bits and pieces of existing templates — or even using their competitors' templates — to generate rules and guidelines. Throughout the last couple of years, it has also become commonplace for businesses to generate AI policies using chatbots like ChatGPT. This often leads to the production of generic guidelines that overlook your company's specific shape and size, including legal and operational requirements, exposing you to compliance gaps and liabilities. While these approaches are fast and cheap, they introduce considerable risk.

Creating an AI policy is not a box-checking exercise. It is a strategic decision. A one-size-fits-all policy can leave dangerous gaps that expose the business to compliance failures, security breaches and even customer dissatisfaction. An effective AI policy requires a human in the loop: a person with experienced judgment who can tailor an AI policy's rules, expectations and guidelines to ensure alignment with the company's business model, values and industry-specific risks.

Creating an effective AI policy starts with an analysis of the company's business model, market position and existing policies. The first step is to analyze the current situation. What are your existing policies? What are your business goals? What are the best scenarios or use cases for AI in your organization? The answers you come up with dictate what kind of AI policy you require — and what needs to go into it. The idea here is that you are actively taking inventory of the opportunities and risks to use AI successfully and safely.

The next step is to initiate policy design. If you have a talented HR leader who is well-versed in the law, privacy and compliance components of AI, work with him (or her) to begin translating your opportunities and risks into rules and expectations around, for example, acceptable use, data handling or employee responsibilities. If you do not have this capability, outsourcing to experts will save you significant time and cost due to the risks of inexperienced policy design.

It is important to provide reasonable notice to employees about the upcoming changes. This can be accomplished by notifying employees that there is a new policy (or update) and the date that it takes effect. From there, your staff will need training on the new AI policy. Depending on jurisdiction, the law, compliance bodies and insurers require that employees are trained and subsequently sign off on the new policies.

Last, but not least, are two additional important steps. First, companies are recommended to continuously monitor and enforce their new AI policies. AI systems change all of the time and so do laws. AI policies can become antiquated rather quickly. Stay on top of changes to keep your organization's use of AI healthy.

Second, communicate with your stakeholders. Let them know you are using AI, or are planning to onboard it. Listen to your employees. Ask for feedback. Hear their concerns. The more you share your plans and visions, the easier it is to both

AI policies are more than just legal documents ... They empower companies to innovate confidently, avoid costly mistakes and build trust with customers.

adopt and manage AI thereafter.

AI policies are more than just legal documents. They are strategic assets. They empower companies to innovate confidently, avoid costly mistakes and build trust with customers. In a market where AI adoption is accelerating, the companies with clear AI policies are the ones that lead. AI is powerful, but only if you have the right blueprint to harness it. ■

Christina Catenacci, BA, LLB, LLM, Ph.D., is a co-founder of voyaige strategy Inc. and a member of the Law Society of Ontario. She is a legal expert in privacy, AI, surveillance and ethics, with experience as a law professor, senior policy advisor and consultant. Her work has appeared in the Montreal AI Ethics Institute's AI Brief, the IAPP's Privacy Advisor, Tech Policy Press and Slaw. Catenacci specializes in privacy laws across Canada, the United States and the European Union, helping organizations develop ethical, tech-driven solutions. She can be reached at christina@voyaigestrategy.com.

Tommy Cooke is a professor, researcher and policy expert specializing in privacy, AI and ethical technology. He earned his Ph.D. in communication and culture in 2017, followed by research fellowships in Germany and at Queen's University, where he won the Wicked Ideas Award. Cooke leads the multinational ADITLom research team on smartphone data privacy and has worked as a policy advisor at the office of Ontario's Information and Privacy Commissioner and as a senior analyst on Deloitte Canada's Trustworthy AI team.

He has published widely on privacy and AI and has taught political science, sociology and engineering.

Cooke can be reached at tommy@voyaigestrategy.com. Visit www.voyaigestrategy.com.

