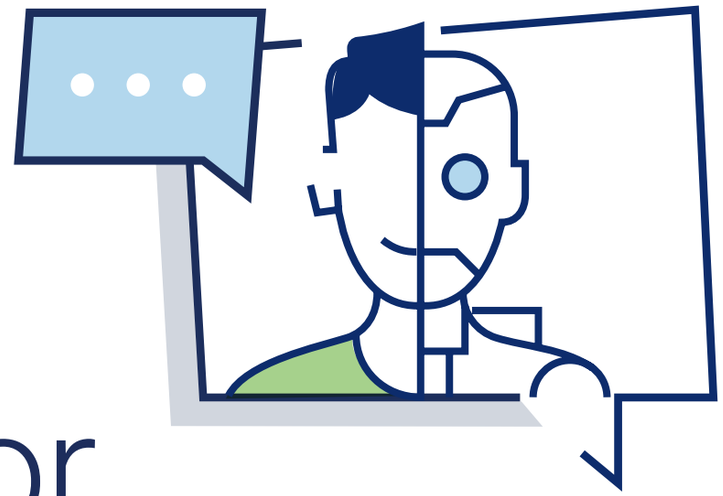
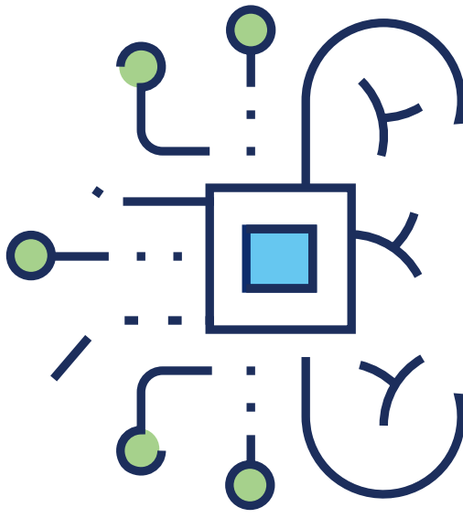
ISACA

# Considerations for Implementing a Generative Artificial Intelligence Policy





An AI Acceptable Usage Policy (AUP) provides organizations with a framework for the ethical and responsible deployment of artificial intelligence. Given the rapid advancements in generative AI, it's important for organizations to provide clear guidance on usage that balances its benefits against risks. ISACA developed this resource as a guide for enterprises to consider when drafting a policy regarding the use of generative AI. Access ISACA's AI resources, including white papers, audit programs, certificates and more, at www.isaca.org/resources/artificial-intelligence.

**Below are key considerations when adopting a generative AI policy.** Please note that the policy should be specifically tailored to meet your organization's unique needs.

## ✓ Who is impacted by the policy scope?

- Consumers will want to know how their information is being managed by AI-driven systems. Regulators may ask if you are adhering to principles of responsible AI. Staff must be informed of the rationale behind this policy and the case for urgency.
- What are your managers, employees, and IT department's generative AI responsibilities?

## ✓ Are the AI systems secure?

- Protect AI systems against unauthorized access, tampering, and misuse. This is especially crucial if the AI system can generate content that could be harmful if misused.
- Before, during and after the implementation of generative AI usage within an enterprise, the systems being used must be proven to be secure and in line with privacy standards.
- It is not the employee's decision to share company data with generative AI tools like ChatGPT. If an organization is committed to providing a safe and secure environment, then any AI used must be shown to be responsible to avoid causing any type of harm. Expectations must be set for the entirety of the organization.
- Establish feedback approach on AI outputs and system performance. Do you trust the system you are employing, the decisions it makes or even the content it generates?

## ✓ Have ethical AI principles been addressed in the policy?

- It is key to ensure generative AI use in your organization does not cause harm, including creating or reinforcing damaging biases. What are the AI ethics and principles your organization must adhere to?
- It is important to have someone within the organization who can explain how the decisions are made by these enabled AI tools or systems. Remaining transparent about these algorithms is essential in retaining digital trust with consumers.

## ✓ What does good behavior look like, and what are the acceptable terms of use?

- Highlighting expectations and acceptable behavior versus unacceptable behavior is an important consideration for creating a policy. For example, AI tools should be limited to business-related purposes while remaining in line with the ethics and privacy regulations of the organization.
- Outlining how AI won't be used is just as important as determining acceptable uses. The context of what is and isn't acceptable is dependent on your industry.

## ✓ What guidelines are in place for data handling and training?

- It's crucial to specify guidelines when sourcing data, particularly when dealing with personal data or sensitive information (e.g., a strong emphasis on the use of de-identified and anonymized data to ensure priavacy). Also, the quality of the data is important, as it directly impacts the accuracy and reliability of the output.

"When creating an Acceptable Usage of Generative AI Policy for your organization, it's crucial to ensure that all relevant stakeholders have a voice in the process. Stakeholders offer technical expertise, ensure ethical alignment, provide legal compliance checks, offer practical operational feedback, collaboratively assess risks, and jointly define and enforce guiding principles for AI use within the organization. Key stakeholders—ranging from executive leadership, legal teams and technical experts to communication teams, risk management/ compliance and business group representatives—play crucial roles in shaping, refining and implementing the policy. Their contributions ensure legal compliance, technical feasibility and alignment with business and societal values."

**MARY CARMICHAEL**
CRISC, CISA, CPA, Member of ISACA Emerging Trends Working Group

## How will this policy encourage transparency and attribution?

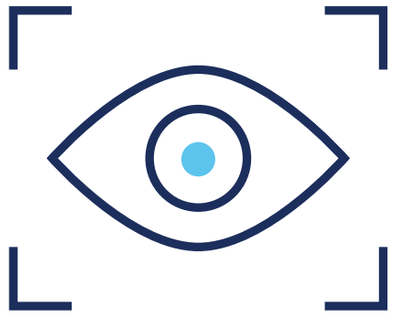
- Is there a mandated disclosure that content has been AI-generated when shared or published? Encourage the use of watermarks or other indicators for AI-generated content.
- Determine responsibility for AI-generated content creation and distribution within the organization. Outline procedures for reviewing and validating AI outputs.

## How will your organization ensure legal and compliance requirements are met?

- Highlight legal and compliance requirements with local, national and international laws, especially concerning copyright, data protection and misinformation.

## What are the limitations and risks involved?

- Acknowledge inherent limitations of generative AI models. Provide guidance on when not to rely solely on AI outputs, emphasizing human oversight.



## How does this policy link to others already in place?

- Bringing attention to how your generative AI policy connects to other policies that are already in place is key in providing stakeholders with a thorough understanding of requirements and expectations. Data privacy and information security policies, for example, are inherently linked to AI policies and must support each other. Stakeholders can benefit from a link to these complementary policies under a “for more information” section.
- Generative AI policies should not be siloed. Collaboration is key because AI impacts the business in different ways. Consider employing an integrated approach to optimize policy coverage.

## How will you highlight exception handling?

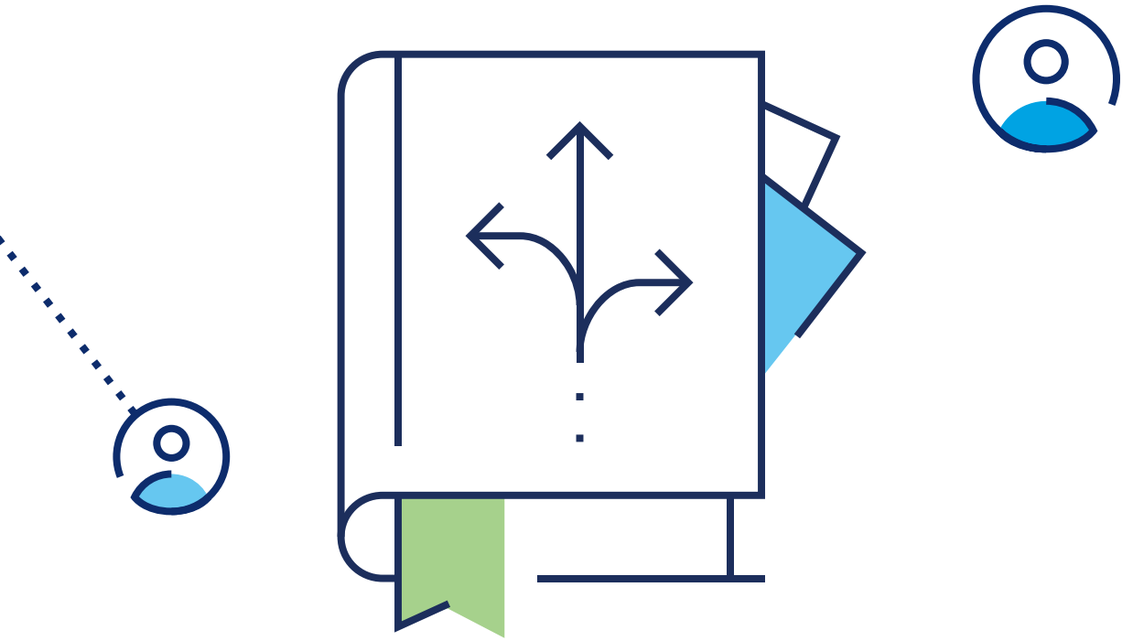
- What will the process look like for unique cases where escalations or exceptions to your AI policy are necessary? In some cases, a generative AI tool may be required for a project or campaign where it usually wouldn’t be allowed—how will approval be determined for such circumstances?

## How will you report and investigate violations?

- Providing IT with the appropriate tools to investigate is critical in the reporting and investigation process. If there is a suspected violation of this policy, it is important to ensure that the appropriate parties have the right to review any AI communications or usage of a generative AI tool.
- Employee codes of conduct and HR policies may already outline relevant penalties for AI violations. Depending on the severity of the infraction, including whether the employee came forward or the violation was revealed in another way, employees may face stunted career growth or termination of their role.

## Who will review, manage and audit?

- Establish who owns the policy, how it will be managed and audited, and how it will be kept both current and working as intended. Risk assessment and other forms of support are essential given the degree of change that will happen in the coming years.
- In the current tech landscape, everyone is interested in AI. This means there is a broader stakeholder base than one might initially anticipate.



## How and when will the policy be updated?

- Once a policy is published, people tend to forget about it. In order to prevent this from happening, stakeholders must be educated and informed, and this knowledge must be constantly reinforced.
- If a new capability for your generative AI tool is released, who will determine how that impacts the policy? What guidance will you provide to staff to ensure a mutual understanding of what is and isn't allowed?
- At least annually, but likely more frequently, this policy should be updated depending on what is occurring within your specific industry and/or organization, especially in terms of deploying new AI capabilities.
- The regulatory environment is changing rapidly, so consider having the appropriate measures in place so that your policy is flexible enough to be relevant in an evolving regulatory landscape.
- Establish an approach to allow stakeholders to provide feedback on the policy, fostering a culture of continuous improvement.

**Learn more at**
**isaca.org/resources/artificial-intelligence**