Shumaker

MAY 8, 2026 | PUBLICATION

Client Alert: AI is Already in Your Organization - Your Acceptable Use Policy Can't Wait

INDUSTRY SECTOR

Technology

RELATED PROFESSIONALS

Nick Carr

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

Whether or not your organization has formally adopted artificial intelligence (AI) tools, the reality is that AI is already being used internally. This article explains what an AI Acceptable Use Policy (AIAUP) is and why every organization needs one. A well-designed AIAUP minimizes risk and establishes a framework for using, adopting, and implementing AI tools responsibly across the organization.

AI Is Already in the Workplace, With or Without Oversight

Once viewed as science fiction, AI is now firmly embedded in everyday life. Whether for work or personal use, people increasingly rely on AI to write, research, and process information faster. Employees frequently use these tools on their own initiative, however, without clearly defined policies or organizational oversight governing their use. AI tools are easy to access, and as teams adopt them independently, blind spots emerge that expose the organization to security and compliance failures. AI adoption inside organizations is outpacing leadership's awareness, and that quiet but widespread adoption is what makes a thoughtful, formal AIAUP a necessity.

The Risks of Ungoverned AI

Without clear oversight, AI use can rapidly amplify organizational risk. The most common issues include exposure of sensitive data, such as when employees input confidential, proprietary, or regulated information into publicly available AI platforms; erroneous or biased AI outputs; threats to intellectual property (IP) protection; and heightened exposure to an expanding regulatory landscape. For example, providing patentable or trade secret information as an input to an AI tool may jeopardize patentability or trade secret protection. AI deployed without governance is a liability, not an asset, placing organizations at risk of security incidents, loss of IP rights, regulatory enforcement, and erosion of trust.

Two emerging risk areas warrant special attention. First, agentic and autonomous AI tools—those capable of independently initiating financial transactions, sending external communications, or modifying systems—can cause significant harm if deployed without managerial approval, human-in-the-loop checkpoints, and tested rollback procedures. Second, generative AI makes it trivial to produce synthetic media, including deepfakes that impersonate real individuals or that infringe publicity, copyright, and trademark rights, exposing organizations to reputational and legal liability if such content is created or distributed without controls.

Elements of an Effective AIAUP

An effective AIAUP should address the following:

1. **State the purpose and scope of the policy.**
   The policy should explain why the organization is adopting an AIAUP and define who and what it covers, including employees, contractors, and vendors using AI for organizational purposes. A clear scope also makes plain that the AIAUP supplements, and does not replace, other applicable policies and legal or contractual obligations.
2. **Clearly assign governance and oversight responsibilities.**
   The policy should designate the individuals or committees responsible for AI governance and define their authority over approvals, monitoring, and updates. Without a clearly named owner, AI-related decisions tend to fall through the cracks between legal, IT, security, and the business.
3. **Establish a tool evaluation and approval process and maintain an approved tools list.**
   Organizations should vet AI tools before they are used, maintain a list of approved tools, and require advance approval for anything outside that list. The evaluation process should weigh security, contractual, legal, and ethical considerations, and the approved list should be revisited periodically as tools and risks evolve.
4. **Define prohibited data and prohibited uses.**
   The policy should identify the categories of sensitive information (such as confidential, proprietary, regulated, or personally identifiable data) that may not be entered into public or unapproved AI tools. The policy should also identify prohibited use cases regardless of the data involved—for example, generating deepfakes or other harmful content, relying on AI as the sole basis for legally significant decisions, or allowing AI tools to take autonomous actions without appropriate guardrails. Setting these boundaries in advance is one of the most effective ways to prevent the highest-risk incidents.
5. **Require ethical use and human review of AI outputs.**
   The policy should set expectations for fair, transparent, and non-discriminatory AI use and require qualified personnel to review and validate AI-generated work product before it is relied upon, shared externally, or used in client deliverables. Where AI assistance materially contributed to an external deliverable, the policy should also require an appropriate disclosure.
6. **Operationalize the policy through training, monitoring, and reporting.**
   The policy is only as good as the infrastructure that supports it. Employees should acknowledge the policy and complete recurring AI training as a condition of access; AI use should be subject to appropriate monitoring; and the organization should provide clear channels for reporting suspected misuse, escalating urgent concerns, and surfacing improvement opportunities, with defined consequences for noncompliance.

Governance Is the Responsibility of Leadership

AI governance demands visible executive leadership, not quiet delegation to IT departments. Executive leadership must set expectations, define accountability structures, and put enforcement mechanisms in place

to ensure responsible AI use across the organization. That leadership posture is what transforms an AIAUP from a static document into a meaningful operating discipline that aligns AI use with the organization's legal obligations, ethical standards, and broader business values.

An AIAUP is no longer optional. Putting one in place now helps organizations reduce legal, security, privacy, and reputational risk, align employees around consistent standards, protect customer and company data, and lay the foundation for responsible, long-term AI adoption. Organizations that act proactively can capture AI's productivity benefits while maintaining the control, transparency, and accountability that today's regulatory and business environment demands.

Shumaker's Technology, Data Privacy, Cybersecurity & AI team regularly advises organizations on developing, implementing, and maintaining AI Acceptable Use Policies tailored to their industry, risk profile, and operations. Please contact us to discuss how we can help your organization put the right framework in place.

Shumaker