Responsible AI: Use Policies and Best Practices

Artificial Intelligence (AI) is transforming the way we work by improving efficiency, enhancing decision-making, and helping teams focus on higher-value tasks. From drafting communications and analyzing data to automating repetitive tasks, AI tools offer significant opportunities for innovation and productivity. However, with these benefits come important responsibilities.

To ensure AI is used safely, ethically, and in compliance with organizational standards, all employees should understand and follow established AI use policies and best practices.

Why AI Governance Matters

AI systems can process large amounts of information quickly, but they are fallible. AI-generated content may contain inaccuracies, bias, outdated information, or unsupported conclusions. In addition, improper use of AI tools can create risks related to privacy, intellectual property, confidentiality, regulatory compliance, and cybersecurity.

Effective AI governance helps organizations:

- Protect sensitive and proprietary information.
- Maintain compliance with legal and regulatory requirements.
- Reduce cybersecurity and privacy risks.
- Promote ethical and unbiased decision-making.
- Preserve customer, employee, and stakeholder trust.

Responsible AI use is not just an IT issue. It is a business responsibility shared by every member of the organization.

Key AI Use Policies

Protect Confidential Information

Never enter confidential, proprietary, client, employee, or regulated data into public AI platforms unless the tool has been specifically approved for that purpose.

Examples of sensitive information include:

- Client records
- Financial data
- Personal identifiable information (PII)
- Source code
- Trade secrets
- Internal business strategies

When in doubt, assume the information is sensitive and consult your organization's AI or data governance guidelines.

Use Approved AI Tools Only
Organizations often evaluate AI tools for security, privacy, compliance, and contractual requirements before approving their use.

Employees should:
- Use only company-approved AI solutions.
- Follow established access controls and security protocols.
- Avoid downloading unapproved AI applications or browser extensions.
- Verify that third-party tools meet organizational requirements.

Allow for Human Oversight
AI should support decision-making, not replace human judgment. The user remains accountable for the final work product.

Always:
- Review AI-generated content before sharing or publishing.
- Validate factual claims and recommendations.
- Confirm calculations, analyses, and interpretations.
- Apply professional judgment when making business decisions.

Respect Intellectual Property Rights
AI-generated outputs may incorporate information learned from large datasets. Users should ensure that generated content does not violate copyrights, licensing agreements, or intellectual property obligations.

Before distribution:
- Verify ownership and usage rights.
- Cite sources when appropriate.
- Avoid presenting AI-generated work as original research without review.

Avoid Bias and Discrimination
AI systems can sometimes reflect biases present in training data. Decisions affecting employees, customers, or stakeholders should be reviewed carefully to ensure fairness and equity.

Pay particular attention to:
- Hiring and recruiting recommendations
- Performance evaluations
- Customer-facing decisions
- Risk assessments
- Eligibility determinations

AI Best Practices for Everyday Use

Be Clear and Specific

The quality of AI outputs often depends on the quality of the prompt. Provide clear instructions, relevant context, and desired outcomes. More precise prompts produce more useful results.

Instead of asking: "Analyze this data."
Consider: "Identify quarterly sales trends, highlight significant variances, and summarize key business insights."

Verify Before You Trust

AI can generate convincing content that appears accurate but may contain errors.

Before using AI-generated information:

- Cross-check facts stated
- Confirm sources and links
- Review assumptions
- Test recommendations where appropriate

Remember: Confidence does not equal accuracy.

Keep a Record of Significant AI Use

For important business decisions document AI usage. Documentation supports transparency, accountability, and audit readiness. Be sure to list:

- Which AI tools were used
- The purpose of the AI assistance
- Key prompts or inputs
- Validation and review steps performed

Apply the Principle of Least Data

Only provide the minimum information necessary for the task. Reducing data exposure lowers risk.

For example:

- Remove personal identifiers where possible.
- Share summaries rather than raw records.
- Limit input to relevant information only.

Understand AI Limitations

AI tools do not possess human understanding, intent, or accountability. They can:

- Hallucinate facts
- Misinterpret context
- Produce inconsistent results
- Generate outdated information

Treat AI as a powerful assistant, not an authoritative source.

A Shared Responsibility
The successful adoption of AI depends on using innovation with responsibility. Every employee has a role in ensuring AI technologies are used securely, ethically, and in alignment with the organization's values.

By following approved AI use policies and embracing best practices, we can use the benefits of AI while protecting our clients, colleagues, and organization from unnecessary risk.

Remember: The Three Golden Rules of AI
1. Protect sensitive information.
2. Verify AI-generated outputs.
3. Maintain human accountability.

AI is a powerful tool, but responsible use is what turns that power into lasting value.

The TWARMF Cyber Risk Services Advisor is scheduling Risk Assessments and Incident Response Plan Tabletop Testing visits for members. To get on the schedule, contact Lee Cain, Cyber Risk Services Advisor at 512-619-1437 or Lee.Cain@sedgwick.com.