Macatawa TECHNOLOGIES | IT Solutions & Support For Business

AI Security & Risk:

How to use AI without putting your business data at risk



AI Security and Risk

How to Use AI Without Putting Your Business Data at Risk

Macatawa TECHNOLOGIES

AI adoption is accelerating rapidly - but most businesses are moving faster than their security posture can keep up with. This guide covers risks your team needs to understand, and the practical steps to use AI confidently and safely.

Key Risks to Understand

Shadow AI

Employees are using AI tools the company hasn't approved. Nearly 50% adopt tools without telling IT or management, and 45% admit to pretending to know how to use AI to avoid scrutiny.

Data Entered Into AI

When data is entered into free or consumer AI tools it is recorded, stored, and used to train the model. Once data is entered it cannot be removed. Meeting transciption and summarizaiton tools are the fastest-growing and most overlooked risks.

AI Hallucinations

AI doesn't retrieve or verify facts - it predicts statistically likely answers and fabricates information when uncertain. AI tools don't say "I don't know". They fill in gaps of information with plausible sounding information.

Comliance Exposure

AI doesn't get a compliance exemption. If you are HIPAA compliant, your AI and any AI used by employees must also be compliant. Financial regulations, and legal standards all apply. If your business has compliance obligations, so do your AI tools.

Consumer Tools vs Enterprise Agreements

Feature	Consumer/Free Tools	Enterprise Agreements
Data Protection Clauses	None gaurenteed	Contractually defined
Your data used for training	Typically yes	Opted out by default
Audit/Compliance Support	Not available	Available
Access Controls	Single sign-on only	Role-based access
HIPAA/Finance Compliant	Not supported	Business Associate Agreement available

AI Security and Risk

How to Use AI Without Putting Your Business Data at Risk

Macatawa TECHNOLOGIES

What Data Is at Risk?

- ✓ Client names, contact info, & contracts
- ✓ Pricing structures & financial data
- ✓ Employee records & HR communications
- ✓ Meeting notes, recordings & transcriptions
- ✓ Internal strategy, roadmaps, & trade secrets
- ✓ HIPAA regulated health information

Guardrails Your Business Should Implement Now

1	**Audit your tools.** Ask your team which AI tools they currently use –approved or not. You cannot manage what you don't know about.
2	**Upgrade to enterprise-grade agreements.** If your team uses AI, ensure you are on a plan that includes data protection clauses and compliance support.
3	**Train your team.** Only 32% of employees have received formal AI training. Training doesn't need to be complex – focus on what AI is good at, bad at, and what data should never enter it.
4	**Establish a human review step.** Any AI output used for client deliverables, financial decisions, or legal documents must be reviewed and verified by a person.
5	**Create a formal AI usage policy.** Define approved tools, prohibited uses, data classification rules, and verification requirements.

AI Security and Risk

How to Use AI Without Putting Your Business Data at Risk

Macatawa TECHNOLOGIES

Why Your Business Needs an AI Usage Policy

An AI usage policy is the foundation of repsonsible AI adoption. Think of it as the equivalent of a computer or internet acceptable use policy – defining what tools are approved, what data is permitted, and what safeguards are required. 56% of employees say they have no clear guidance on AI usage. That gap is a liability sitting on your desk.

The 5 Core Components of the Policy

1 **Approved Tools List**
Define which AI tools are sanctioned for use, by which roles, and for which tasks. Any tool not on the list requires IT approval before use.

2 **Data Classification Rules**
Specify clearly what data may and may not be entered into AI. No client PII, financial records, health data, or proprietary strategy should be entered into consumer tools.

3 **Verification Requirements**
All AI-generated output used in client work, financial reporting, or legal documents must be reviewed and verified by a human before use or distribution.

4 **Prohibited Uses**
No sensitive data in consumer-grade tools. No AI used for regulated decisons without human review. No AI-generated content presented as orginal without disclosure.

5 **Mandatory AI Training**
Employees must complete baseline AI training before using AI for any work. Training should cover: what AI does well, what it gets wrong, and what data to protect

AI Security and Risk

How to Use AI Without Putting Your Business Data at Risk

Macatawa TECHNOLOGIES

Sample AI Usage Policy – Template

PURPOSE	This policy establishes guidelines for the use of artificial intelligence (AI) tools by employees of [Company Name] to protect sensitive data, ensure compliance, and promote responsible AI use.
SCOPE	Applies to all employees, contractors, and third parties who access company systems or handle company data.
APPROVED TOOLS	Approved AI tools: List tools. Any tool not listed requires written approval from IT before use.
PROHIBITED DATA	The following may NEVER be entered into any AI tool without explicit written approval: Client PII, financial records, pricings, or contract terms, health or HIPAA regulated data, proprietary strategy, trade secrets, or unreleased products, employee records or HR communications.
VERIFICATION REQUIREMENT	All AI generated content used in client deliverables, financial reporting, or legal documentation must be reviewed and verified by a human before submission or distribution.
TRAINING	All employees must complete [Company Name]'s AI Training before using AI tools for any business purpose. Training must be refreshed annually.
VIOLATIONS	Violations of this policy may result in disciplinary action up to and including termination. Data breaches resulting from policy violations may be reported to relevant regulatory authorities.
REVIEW CYCLE	This policy will be reviewed and updated at annually or when significant AI regulatory changes occur.

READY TO ASSESS YOUR AI READINESS? Reach out to us today!

www.macatawatech.com sales@macatawatech.com 616-394-4940