



AI Security Best Practices

Incorporating AI into your workflows can be transformative, but safeguarding data privacy is essential. Here are some best practices to ensure the secure and responsible use of AI tools like ChatGPT:

Use Caution When Sharing Sensitive Details

01

When using AI for tasks like financial analysis, ensure data privacy by taking the following precautions:

Avoid sharing full sets of confidential or sensitive information, such as unmasked personally identifiable information (PII), raw financial data, or trade secrets.

Wherever possible, anonymize or aggregate data before inputting it into the AI system. For example, use placeholder names, round figures, or generalized metrics instead of precise details.

Implement Secure AI Tools for Financial Analysis

02

If your organization requires AI for analyzing financial data, consider tools specifically designed for secure financial use cases. These tools should meet strict security standards, such as data encryption, compliance with financial regulations (e.g., SOC 2, GDPR), and the ability to operate within a closed system.

Understand Privacy Policies and Security Protocols

03

Ensure that any AI tools used for financial analysis provide transparency about how data is processed and stored. Opt for solutions that offer robust security features, such as on-premise deployment or private cloud options, to protect sensitive data.

Minimize Risk During Analysis

04

For financial analysis, limit the amount of raw data shared with the AI at any one time. Instead, provide summarized or segmented data points that can still yield actionable insights without compromising security.

Review Outputs Carefully

05

When using AI for sensitive applications like financial analysis, ensure that outputs are reviewed and validated by a qualified individual. This mitigates the risk of inaccuracies or potential exposure of sensitive insights.

By following these practices, you can harness the power of AI while maintaining trust and safeguarding sensitive information.