AI DATA PRIVACY AND CONFIDENTIALITY

AI tools are transforming the way professionals analyze data, generate content, streamline workflows, and make strategic decisions. These powerful technologies can elevate organizations' productivity and innovation, but they don't come without risk. When using AI tools, keep data privacy and confidentiality in mind.

AI AND YOUR DATA

AI tools rely on large data sets to learn, detect patterns, make predictions, and generate meaningful insights. Queries submitted to these tools may occasionally contain highly sensitive information, such as financial records, trade secrets, and personal health information. User data can also be collected, raising important privacy and confidentiality considerations.

MAKING INFORMED DECISIONS ABOUT AI

There is a potential tradeoff between allowing AI systems to fine-tune on your data to improve output versus the potential exposure of that data. To use AI responsibly, understand what data is collected, why, and our organization's data policies. This awareness helps you make more informed decisions with regards to balancing convenience with privacy and confidentiality risks.

KEY AI PRIVACY AND CONFIDENTIALITY RISKS

- **Data leakage**

AI tools can unintentionally expose confidential information, leading to data leaks that pose serious compliance and reputational risks for organizations. Data leakage can occur due to a lack of awareness about organizational policies and what data can safely be entered into AI tools. A common mistake is using unapproved tools to summarize or write emails, unintentionally exposing all email content to the tool.

Signs of data leakage include:

  - Users, customers, or employees reporting that their personal data has appeared in unexpected places.
  - Claims that data is being used in ways not originally disclosed or authorized.

- **Cyberattacks**

One common tactic involves attackers feeding misleading data into an AI model to manipulate its decisions, resulting in unreliable outputs.

Signs that a system has been compromised include:

  - Sudden changes in performance like frequent system crashes, unusual error messages, or forced shutdowns.
  - Unusual or inconsistent results.
  - Drops in accuracy, or predictions that seem out of the ordinary.

USING AI SECURELY AND RESPONSIBLY

Implement the following best practices to protect your data and confidentiality:

- Stay informed about current and emerging AI-related cyber threats.
- Follow organizational guidelines on how to handle sensitive data.
  - Use only approved third-party AI service providers that have been vetted for their security controls and compliance with relevant regulations.
- Know your organization's Data loss prevention (DLP) policy.
  - Understand what data can be uploaded and processed in AI systems and how the system protects and uses the data.
  - If an incident occurs, or you notice suspicious behavior, report it immediately to the relevant departments. This could include IT, Legal, HR, or public relations teams.

Awareness of privacy and confidentiality concerns empowers you to harness the power of AI, safely!