# Using AI Assistants Securely

## AI tools make work faster.

**But, they can also put data at risk.**

Many AI-powered tools and large language models (LLMs), such as ChatGPT, Gemini, and Claude, retain the information you enter as part of their dataset. If sensitive or confidential data is shared without safeguards, it could be exposed beyond your company's control, creating security, privacy, and compliance risks.

Additionally, unapproved tools may not meet organizational security requirements, and AI-generated outputs must be reviewed for accuracy and bias before use.

For these reasons, secure practices are essential when using AI in the workplace.

## Work smart. Stay secure.

**Take steps to keep company data safe.**

### Protect What You Share

If you wouldn't share the information outside your company, don't enter it. Never share sensitive or confidential data with LLMs. Remove identifiers and only use company-approved platforms with strong account security, including multifactor authentication (MFA).

### Configure Privacy Settings

Many AI platforms include privacy and data sharing controls that allow you to limit how your information is stored or used by third parties. Where possible, disable settings that allow prompts or conversations to be used for model training and turn off data sharing and history features.

### Verify Before Use

AI-generated content may contain errors, outdated information, or bias. Always review outputs carefully and confirm accuracy before use. Employees are responsible for any work produced using AI tools.

## Security starts with you.

**Use AI responsibly and securely.**