

AI Use Policy

Owner: Dana Whitfield, IT Director **Effective:** October 1, 2026 **Next review:** April 1, 2027

1. Why this policy exists

AI tools help us draft, code and analyze faster, but anything typed into them can leave our control. This policy protects customer payment card data under PCI DSS, our designs and pricing, and our coworkers' personal information, so everyone at Example Manufacturing Co. can use AI with confidence.

2. Approved tools

Microsoft 365 Copilot: Drafting emails and documents, summarizing meetings, and working with company files in Word, Excel and Outlook.
ChatGPT Enterprise/Team: Drafting, brainstorming, research and code help, using your company-issued account only.

Sign in with your company account, never a personal or free account. Any other AI tool, plugin or browser extension needs approval first, even if you already use it.

3. What you can put where

✗ Never in any AI tool

- Payment card numbers, security codes or other cardholder data
- Passwords, API keys, or network and machine credentials
- Employee Social Security numbers, medical or payroll records
- Customer files whose NDA forbids sharing with outside services

• Only in approved tools

- Internal drawings, specs and manufacturing process documents
- Customer names, orders, quotes and pricing
- Source code, scripts and PLC programs
- Supplier contracts and cost data

✓ Fine in any AI tool

- Public product catalog or website text
- General questions about Excel formulas or industry terms
- Brainstorming generic ideas like safety poster slogans

4. Your responsibilities

- Move work off personal AI accounts and use only the approved company tools.
- Check the data tiers before pasting anything into an AI tool.
- Review every AI output for accuracy before you send, ship or build from it.
- Never let AI make final decisions on safety, quality, hiring or payments.
- Report mistakes or suspicious tool behavior right away.

5. Asking for a new tool

To ask for a new AI tool, email ai-requests@example.com with the tool name, what you want to use it for, and what data it would touch. You will get an answer within two weeks.

6. If something goes wrong

If you put restricted data into an AI tool or spot a problem, tell Dana Whitfield, IT Director, right away at [IT security contact email or phone]. Fast reporting limits harm and will not get you in trouble. Violations start with a conversation with your manager; HR is involved only for repeated or serious cases.

7. Monitoring

AI use on company devices and accounts is monitored to protect company and customer data, consistent with our other IT policies.