

# AI IN THE WORKPLACE:

## What Your Business Should (*and Shouldn't*) Be Doing!

Artificial Intelligence tools are already inside your business, whether you planned for them or not. Employees are using them to draft emails, summarize documents, and speed up daily tasks.

**The question is no longer whether your team will use AI. It's whether they're using it safely.**

### What Your Business *Should* Be Doing

- Stick to IT-approved AI tools. Free, unvetted apps often store or reuse the data you enter.
- Set a clear AI use policy. Employees need to know what's allowed and what isn't.
- Classify data before it goes into a prompt. Client records, financials, and internal documents should never be pasted into a public AI tool.
- Review AI-generated work before it goes out. Treat it like a draft from a new employee, not a finished product.
- Loop in IT before adopting new tools. A five-minute check can prevent a real exposure.

### What Your Business *Shouldn't* Be Doing

- Don't assume "free" means "private." Many free AI tools use your inputs to train their models.
- Don't let shadow IT take over. If employees are using AI tools IT doesn't know about, you have no visibility into what's leaving your network.
- Don't skip the policy because it hasn't been a problem yet. One exposed file is enough to cause lasting damage.
- Don't treat AI oversight as an IT-only issue. Every department that touches client or company data needs to understand the risk.
- Don't wait for a breach to take this seriously.

NOT SURE  
WHERE YOUR  
BUSINESS  
STANDS?

Directive can walk you through it. Contact us for a free AI Consultation and get a clear read on what to fix first.