

What NOT to Put in a Skill

A governance-minded look at the limits

The Core Idea

A skill remembers instructions, not secrets. Treat SKILL.md like a shared playbook — something any coworker could read — not a private vault.

Keep This Out

1. Passwords, API keys, or account numbers.
2. Personally identifiable client or customer data.
3. Anything you'd be uncomfortable with a coworker reading verbatim.
4. Company policy language you didn't write — link to the real policy instead of restating it.

THE HANDOFF TEST

If you'd be fine with a new hire reading your SKILL.md on day one, it's clean. If not, rewrite it before you save it.