



Three rules for any AI in your business.

Write them down before you connect an AI agent to anything. Fill in this page once, and change it when the job changes.

The template

The job: _____

Rule 1

What it can touch

Write down every app and folder it can open. Read-only wherever you can. Start with one inbox, and add the next app when you trust it.

App or folder: _____ Read-only or can change: _____

App or folder: _____ Read-only or can change: _____

App or folder: _____ Read-only or can change: _____

App or folder: _____ Read-only or can change: _____

Rule 2

What it asks first

Anything that leaves the business waits for your OK: a message, a post, a payment. It can draft all day. You still press send.

It asks me before it: _____

It asks me before it: _____

It can do on its own: _____

Rule 3

Where it writes it down

Every action goes in one log, with the time. You read it once a day. If something goes wrong, the log tells you where to look.

The log is kept in: _____

I read it every day at: _____

Last changed on: _____

Fill it in with AI

Paste this into ChatGPT or Claude before you connect anything. Fill in the job.

Copy this

Paste into ChatGPT or Claude

I want an AI agent to do one job for my business: [the job]. Help me write its three rules: what it can open, what it must ask me before it sends, posts or pays, and where it logs what it did. Ask one question at a time. Then give me the rules on one page.

- Answer with the real names of your apps and folders.
- If a rule feels too loose, ask it: “What could go wrong with this rule?”
- Copy the answers into the template and keep the page.

Why write them down now

As of October 2026, OpenAI has told more than 100 organizations that its agents may have gone into their systems without permission. Meta's new Muse for Small Business (US and Canada only) promises that nothing sends, posts or spends without your approval. Your agent needs the same limits, on paper, before it starts.

The three rules at work

This is an example log of how my AI operators work. They're already working for estate agencies in Spain.

Time	What happened
09:02	A known contact writes. It stays quiet.
09:15	A new enquiry comes in. It drafts a reply.
09:16	The draft waits for the broker's OK.
09:20	Sent, and written to the log.

What this page can't do

A page of rules doesn't stop an agent by itself. Set the same limits in the tool's own settings, where it lets you, and read the log. This page isn't legal advice on contracts or data.

Your next step



New to AI? Start with my free guide “Your first small step with AI” at inikolovai.substack.com.

Questions? Message me on Instagram, @inikolov.