CHECKLIST · BEFORE THE FIRST NODE

YOUR FIRST AGENT

What to decide before you build, the smallest build that is still real, and how to know the agent stayed inside its lines.

SIX THINGS TO WRITE DOWN FIRST

An agent is a program that chooses its own next step. Everything that goes wrong with one traces back to a choice nobody bounded. Bound them on paper before a single node is placed.

- [ ] **One job, one sentence**
  Write what the agent is for in a single sentence. If the sentence needs the word "and", that is two agents.

- [ ] **One trigger**
  What starts a run: a form, an email, a schedule, a message in a channel? Pick one. Everything else waits for version two.

- [ ] **What it may read**
  List the sources by name: this inbox, this folder, this table. Nothing not on the list.

- [ ] **What it may write**
  List the actions: send, create, change, delete. Each one is a place it can do damage, so each one earns its place.

- [ ] **What it may decide alone**
  Which choices does it make by itself, and which does it hand to a person? Anything that spends money or leaves the building goes to a person.

- [ ] **How you will know**
  What does a run leave behind: a log line, a message, a row in a sheet? If you cannot see a run, you cannot trust it.

THE SMALLEST REAL BUILD

Five nodes. Every agent on the show starts this shape; the good ones stay close to it.

1	2	3	4	5
Trigger	**Gather**	**Think**	**Act**	**Report**
The one event that starts a run.	Read only. Pull exactly the sources on your list.	The model, with a prompt that names the job and the limits.	One action from your write list. One.	Tell a person what it did, every run, somewhere they look.

WHILE YOU BUILD

- Use test data until the last step. A real inbox is not a sandbox.
- Give the agent its own credentials, with the smallest access that does the job. Never your own login.
- Put an off switch where you can reach it in ten seconds: a workflow toggle, a revoked key.
- Run it twenty times and read every result before you let it run unwatched.
- Widen one permission at a time, and only after the runs are boring.

SIGNS IT IS DRIFTING

- It did something you did not ask for, even something helpful.
- A run takes far longer than the others.
- The output changes shape: a new format, a new tone, a new field.
- It acted on the wrong record, or on more records than the trigger named.
- It touched a source that is not on your read list.

WHEN IT GOES WRONG

- Stop it. Keep the logs. Read the whole run.
- Fix the boundary first, the prompt second.
- Run the twenty again before it goes back on.