PremiumOps.ai

FREE HANDBOOK

Lead your agents: a starter handbook

My rules for leading a team of AI agents.

By Taina Pereenniemi, PremiumOps

1
A role, a boss and a mandate

2
One shared operating system

3
Fix the system, not just the work

01 · INTRODUCTION

Leading agents is a leadership skill

Social media turned everyone into a brand. AI is turning everyone into a leader.

Most people use AI like a clever search box. You ask, it answers, you fix the answer. That works for small tasks. It does not scale.

Once you have several agents doing real work, the problem changes. It's no longer “how do I write a better prompt?” It's “who does what, who checks it, and who decides?” Those are leadership questions.

> **Tomorrow's winners won't have the best model or the best prompts. They'll know how to lead agent teams.**

Start with the rule that hurts most today.

INSIDE

01 Leading agents is a leadership skill
02 Rule 1: A role, a boss and a mandate
03 Rule 2: One shared operating system
04 Rule 3: Fix the system, not just the work
05 Governance for agent teams
06 The tools we love
07 Our services
08 What clients say

THE THREE RULES AT A GLANCE

Three rules for leading agent teams

1 Every agent gets a role, a boss and a mandate.

What it decides on its own, what it proposes, and what stays with you.

2 Give everyone one shared operating system.

One place for knowledge, goals, roles and rules, work, decisions and memory, for people and agents alike.

3 Agents will make mistakes. Fix the system, not just the work.

Let agents check their own work, and have them suggest improvements.

Same with people. Along the way, short notes show how the same ideas work for human teams too.

02 · RULE 1

Every agent gets a role, a boss and a mandate

I see too many people try to build one giant agent that handles everything. I understand why: it feels simpler. But it rarely works well.

Context is limited

An agent can only keep so much in mind at once. Give it every job and it does each one with less of the context it needs.

Permissions should be narrow

Not every agent needs every permission. The agent drafting your posts doesn't need access to your invoices.

Models differ

Agents don't all need to run on the same AI model. Pick the one that suits the job.

You get much better results when you build a team of agents, each specialised in a different role. Each one gets the context, the access and the model its job needs, and nothing more.

> **One specialist per role beats one assistant for everything.**

What it means

Most failures in multi-agent setups come from unclear scope, unclear ownership or too much access. Give each agent three things, in writing.

A role	Explains what the agent is for: its purpose, what is in and out of scope, the inputs it works from, the outputs it owes and what done looks like. Sometimes that is one line, sometimes a page. It also lists the tools and data the job needs, and nothing more. When an agent's instructions or toolset start to sprawl, split it into specialists.
A boss	Every agent reports to one owner, human or agent. The owner assigns work, reviews output, approves what needs approval, and is who the agent escalates to when it's stuck, unsure or about to do something risky. Feedback is written back into the agent's instructions, so a correction made once sticks.
A mandate	The governance rules. Access follows least privilege: read what it needs; write, change or delete only where its job requires it. Two tiers of action: what it does on its own (low-risk, easy to undo) and what goes to a human for approval (anything external, costly or irreversible, such as sending, deleting, paying or granting access). Every action is logged so it can be audited.

These are typical rules. Each business draws its own lines.

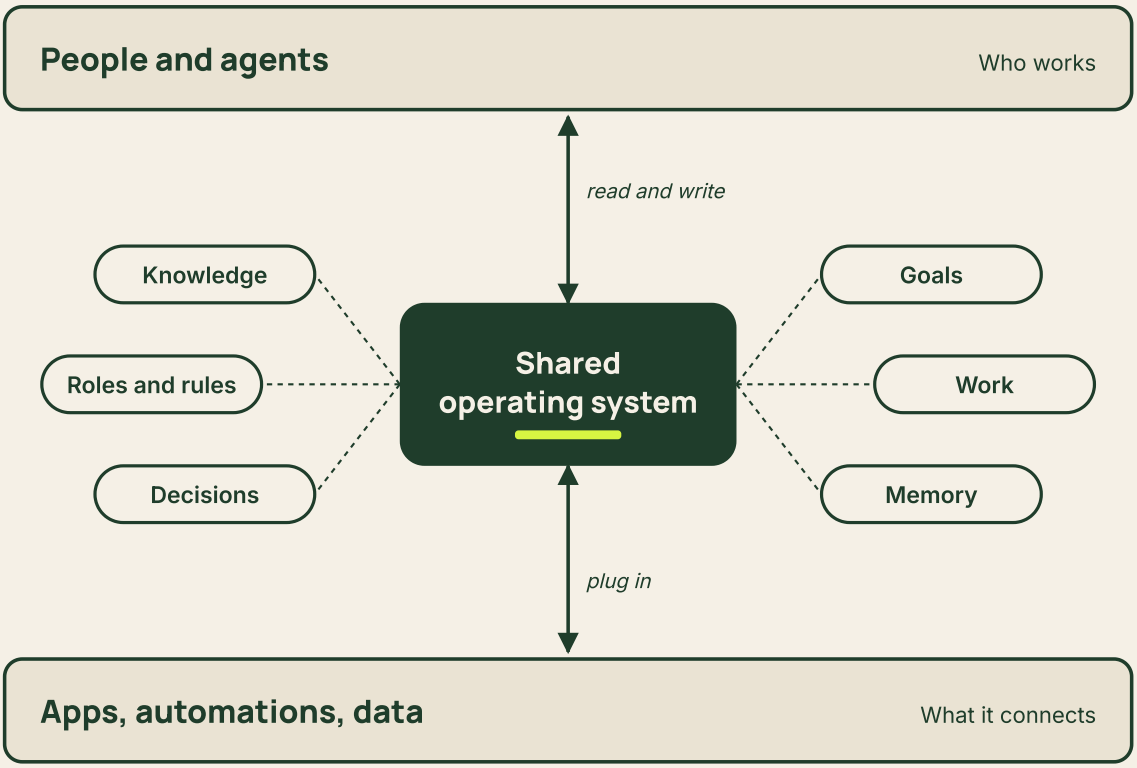
03 · RULE 2

Give everyone one shared operating system

What it means

Agents only know what you give them. If your knowledge sits in ten apps and three people's heads, every agent works from a different picture.

So give everyone, people and agents, one operating system. Think of it as three layers:



Knowledge: how you work, your services, your clients.

Roles and rules: each agent's role and mandate from Rule 1, and the rules everyone follows.

Decisions: what was decided, when and why.

Goals: what matters now and this quarter.

Work: projects and tasks, and who owns them.

Memory: what happened before, so nobody starts from zero.

The shared operating system sits in the middle. People and agents read from it and write to it. Apps and automations plug into it. At PremiumOps, this is Notion.

> SAME WITH PEOPLE
>
> People do better work when answers are written down in one place, not stuck in someone's head. A shared operating system makes onboarding a new person as easy as onboarding a new agent.

04 · RULE 3

Agents will make mistakes. Fix the system, not just the work.

What it means

When an agent gets something wrong, the quick fix is to correct the output yourself. Do that every day and you become the bottleneck. You're the hero again.

Instead, ask: why did it get this wrong? Usually the cause is in the system. A missing piece of context. A rule that's unclear. A role that's too wide. Fix that, and the mistake stops coming back.

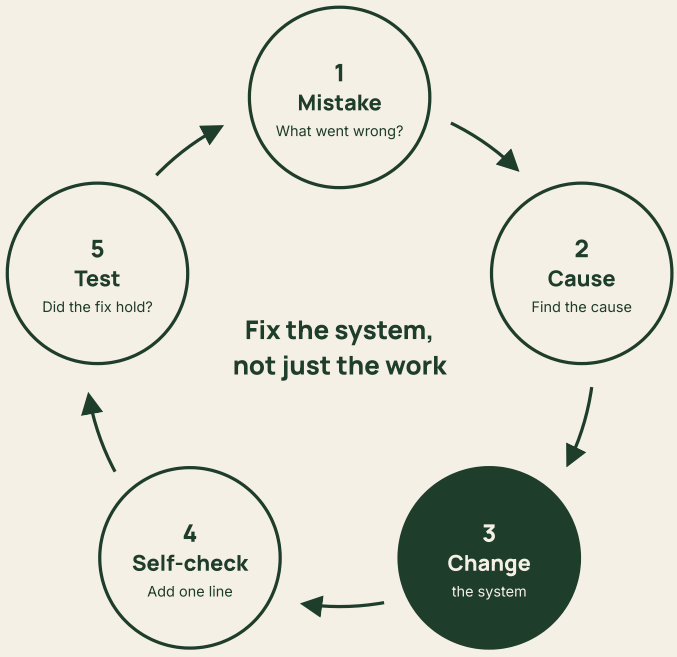
TWO MORE HABITS MAKE THIS WORK

Let agents check their own work.

Give each one a short checklist to run before it hands anything over.

Have them suggest improvements.

Ask agents to tell you what slowed them down and what they would change, without waiting to be asked.



SAME WITH PEOPLE

When a person gets it wrong, the first question isn't “who?” It's “what in our setup let this happen?” Fix that, and the whole team gets better, not just one person.

05 · GOVERNANCE

Setting rules for an agent team

Governance sounds heavy. For a small or medium-sized business it comes down to three questions: who owns what, what an agent may do on its own, and how you know what happened.

There is no single right answer. The rules, and the way you arrive at them, differ from team to team and business to business. A small agency and a regulated finance firm will draw very different lines. But some good practice holds almost everywhere:

Start from the business, not the tech.

Map how work actually flows, decide who owns each area, and only then decide where agents help. An agent added to a process nobody owns tends to make it messier.

Give every agent a role and an owner.

Each agent has a defined job and one owner, a person or a lead agent, who assigns its work and reviews it.

Grant only the access the job needs.

This is least privilege. An agent that only drafts posts doesn't need your invoices. Read access is often enough; write and delete rights are given only where the job needs them.

Sort actions by risk.

Low-risk work that is easy to undo, the agent does on its own. Anything external, costly or irreversible, such as sending, paying, deleting or granting access, waits for a human to approve.

Keep a record.

Log what agents did, so you can check their work, trace a mistake back to its cause and show others what happened.

Start narrow, widen with trust.

New agents begin with fewer permissions and more approvals. As an agent proves reliable at a task, you can give it more room for that task.

One more habit ties it together: review agent work regularly, and when something goes wrong, fix the instruction, rule or access that allowed it, not only the output.

> None of this is new thinking. It matches public guidance such as Anthropic's *Building effective agents*, OpenAI's *A practical guide to building agents* and the OWASP Top 10 for LLM applications, which names *excessive agency*, giving an AI system more functions, permissions or autonomy than it needs, as one of the main risks.

05 · GOVERNANCE

How we do it at PremiumOps

This is one example: our own setup. It suits a small studio where the founder works closely with a team of agents. Yours may look quite different.

Every agent has a role

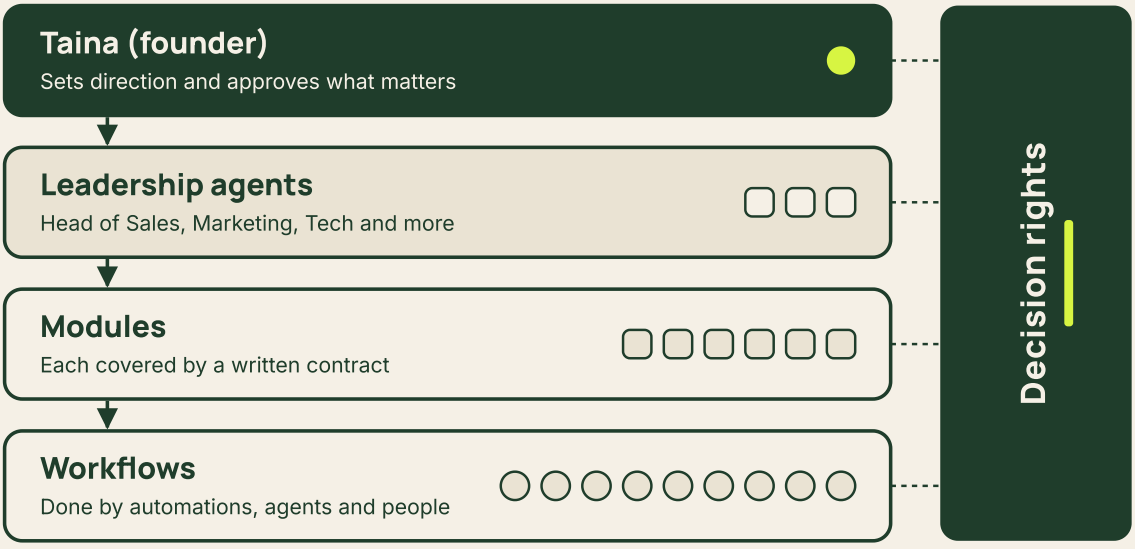
We wrote down a role for each agent: what it is for, what it should and shouldn't do, and which actions need my approval first.

The business is mapped into modules

We mapped the whole business into modules: selling, onboarding a client, delivering a project, marketing, finance and admin, and the tech behind it all.

Each area has a lead agent with a contract

Each group of modules is owned by an agent on our leadership team, such as our Head of Sales, Head of Marketing and Head of Tech. Each one has a written contract that says which modules it covers, what it is responsible for and what it hands over. Agents work within that contract, and I make the final calls.



In practice, agents research, draft and organise on their own. Anything that goes to a client or the public, costs money, deletes something or gives someone access comes to me first. Emails wait as drafts in my inbox until I send them. None of this is fixed: when an agent proves reliable, it gets more room, and when something goes wrong, we fix its contract or instructions.

06 · TOOLS

The tools we love

We help clients with a wide range of tools. These three are our favourites for running a business together with agents.



Notion

The operating system, or company brain.

One place for context, documents, databases, tasks and decisions, which people and agents both read and write. Structured databases give agents reliable context to work from and one shared source of truth, so everyone works from the same picture. Permissions control who can see and change what, and page history shows what changed and when.



Grok Bot

Where our agent team runs.

A team of persistent, named agents, each with its own role, memory, skills and routines: work that runs on a schedule or when something happens. Connectors link them to the tools the business already uses. You manage them in chat, much like teammates, and they can use their own computer and browser for tasks that need one. They ask for approval before sending anything.



Wispr Flow

Voice dictation across your apps.

You speak and it writes the text in whatever app you are using. That lets you give agents instructions, feedback and briefs at speaking speed. Agents do better work with rich context and frequent feedback, and talking makes both practical. I dictate all my messages.

07 · SERVICES

Our services

This is how I run PremiumOps, and how we help clients run on systems, not heroics.

Agentified operating systems

Run your operations on agents and automations, with people approving the steps that matter.

Company brain

Organise your company's knowledge so AI tools have the right context.

Notion consulting

Set up and improve your Notion workspace with the #1 rated certified Notion consultancy.

Grok Bot consulting

Set up Grok Bot agents for your team and learn to run them well.

#1

Rated Certified Notion Consultancy Globally

150+

clients served across the US and Europe

If you'd like a second pair of eyes on your setup, book a call.

Book a 30-minute call

cal.com/premiumops/discovery-call

Taina Pereenniemi, PremiumOps

08 · TESTIMONIALS

What clients say



"...automations save us hours every day and prevent critical steps from falling through the cracks."

Shawna, Dash Media



"She listened carefully, understood our operation, and translated that understanding into practical solutions."

Marianthi, OCM Group



"...has already had a huge impact in helping our operations."

Martin, Telos Education



"This is the best investment we've ever made into our internal process!"

Angel, GreaterThan



"We are a growing organization with ever-changing needs and Taina + Kim were truly our perfect match for our Notion build."

Katelyn, Wondermind



"I've had a whole business system built by her and it's changed my business as well as clearing up my personal headspace."

George, Eagle & Beagle



"She was very clear and professional in her communication, what to expect when and often thought outside of the box."

Marieke, Adverge



"...her deep knowledge of the tool was evident throughout, making our interactions incredibly informative and engaging."

Neha, Metacore

PremiumOps.ai

Systems, not heroics.

If you'd like a second pair of eyes on your setup, book a call.

Book a 30-minute call

#1 Rated Certified Notion Consultancy Globally.
150+ clients served across the US and Europe.

premiumops.ai