

THE TRUST PACK

Your files, and what we answer for, in writing.

For IT, security and procurement teams.

The questions a buyer's IT, security and procurement teams ask first, answered in writing, so they can be checked and kept. Every line here is also on our website, on the pages about your files and security and what we answer for. Where something is not in place yet, this pack says so.

- | | | | |
|----|--------------------------|----|----------------------------------|
| 01 | In three lines | 02 | Your files and security |
| 03 | What we answer for | 04 | Who works on your system |
| 05 | Our own AI policy | 06 | What you own |
| 07 | What is in writing first | 08 | The company, and who to write to |

01 In three lines

Your files can stay in your office.

On one machine you own, if you choose it, where no vendor's cloud holds them.

Every account is in your name.

From day one. Stop any month and keep everything.

No outside model learns from your files.

Your data trains only your own model, with your written yes, and never anyone else's.
Nothing reaches another client.

02 Your files and security

In the order your IT will ask.

2.1 Where does it run?

On one machine you own, in your office, if you choose it. Not in our cloud, not in anybody's cloud. The record, the workflow, the documents and the models that read your mail are built to run on that box, on your network. No vendor data centre holds your files, so there is no vendor data centre for your client to audit.

The machine is small: about the size of a thick book, drawing under 200 watts. It needs a cooled room and a small battery, and it is set to come back on by itself after a power cut.

If you would rather not have a machine, the agents can run in accounts in your firm's own name instead, with the same log, the same yes and the same stop switch. We tell you plainly what that changes about where your files sit before anything is built.

Where this stands today. No client machine is installed yet. Answers 01 to 04 say how the machine is built to work, and on install day we prove each one in front of you and write the receipt into your log. Our own machine runs our own AI work: six kinds of it were checked on 22 September 2026, and that story is on our work page.

2.2 What leaves the building?

Three things, by design. On install day we show you each one.

A heartbeat, once an hour, going up. It says the box is alive, which versions it runs, how many jobs ran, how many are waiting, how many errors, the disk and the temperature. It carries no name, no document and no line of any job.

Signed updates, on a schedule, coming down. Each one is a sealed package checked against our signature before it is allowed to run, pinned to an exact version. The box is built to run its own health checks after an update and to put itself back on the previous version if they fail.

The nightly backup, going out already sealed. It is encrypted on the box before it leaves, to a bucket in your own country, so the bucket holds bytes nobody can read without your key.

Nothing else leaves on its own. Your rate cards, your records, your customers' addresses, passports and photographs stay on the box.

Messages your agents send and receive on WhatsApp, mail or SMS go through those services, as they do today. Your proposal names each one.

2.3 What is encrypted?

The whole disk, all the time. If the machine were carried out of your office, nothing on it could be read.

One catch: an encrypted disk normally needs somebody to type a password when it starts, and a box that waits for a person at three in the morning stays down. So no password is typed. The key is sealed into a small security chip on the machine's own board, and the chip only hands it back when the same machine starts with the same startup files. Lift the disk out and put it in another machine and it opens nothing. One written recovery phrase exists for the day the board itself has to be replaced. It lives in your own password store, never on our side.

On install day we prove both halves in front of you and write both receipts into your log. We pull the power at the wall and watch the box come back on its own. Then we start it once with a tampered startup file and watch it refuse.

2.4 Who can get in?

Your people, on your office network, and on a private network for phones outside the office. Nothing is exposed to the open internet.

Us, only for support, over that same private network, and only the people named in your proposal. Every support session is recorded on your box, by your box, and the recording is yours. Nothing is ever downloaded from your machine.

Nobody else. Nobody outside the names in your proposal, no model vendor and no analytics company. The models run on your box, so there is no third party reading your mail to answer a question about it.

2.5 **What does it write down about itself?**

Every step records what it read, which tool or model ran, what came back, how long it took, and who, if anyone, said yes. That log is append only and it is yours. It is what makes an audit a morning's reading instead of a project.

It is kept for at least 180 days, the period India's CERT-In directions set for a company's logs, on the machine in your own office. It can be kept for longer, and a copy can go to your own monitoring.

2.6 **Does any model learn from our files?**

No outside model does. Your data trains only your own model, with your written yes, and never anyone else's. A model trained on your files runs on your machine or in your own accounts, and it is yours.

With the machine, the models run on the box itself, so no model vendor reads your files at all. Without the machine, we tell you plainly which provider reads what before anything is built, and it is written down.

2.7 **Does anything reach another client?**

No. Agentec is its own company. Nothing you give us reaches IKAN, the firm our founder also works for, or any of our clients, and your files are never used to build for anyone else.

2.8 **Which data laws does it meet?**

Most data laws start with three questions: who holds your people's data, where, and who else reads it. With the machine, you hold it, in your own office, in your own country, and no model vendor reads it. The nightly backup is sealed before it leaves and goes to a bucket in your own country.

We do not give legal advice. In the session we go through what your own law asks of you, India's DPDP Act, Singapore's PDPA, the UK GDPR or any other, and what is agreed is written down before anything is built.

2.9 If something goes wrong?

Your own system alerts your named person at once, at any hour. It never waits for a message from us. India's CERT-In directions give a company six hours from noticing an incident to report it, so the alert reaches you first, from your own system.

If we notice something first, we tell your named person what we know within six hours of noticing, any day, with every fact you need to make your own report to CERT-In in time. Out of our support hours an agent that stops stays stopped, and your team works the old way until we are back. What happens when an agent gets a job wrong is on what we answer for.

2.10 Which certificates do you hold?

We do not hold ISO 27001 or SOC 2 yet. We say so rather than print a badge.

What we can show you now. This page and the trust pack, in writing and dated. Our own AI policy, in six lines. Our own machine at work, with the six kinds of AI work checked on it on 22 September 2026. The audit that checks every automation on our own machines each night, and the guards that watch them, both on our work page with their dated counts.

What is not there yet. A security test by an outside auditor, and the receipts from a client's install day. When either exists, its date goes on this page.

2.11 What changes for a larger firm?

The same rules, sized to you. For a firm of thousands, the proposal sets each of these out in writing before anything is built.

Where it runs. In your own cloud account or your own data centre, sized to your load, where one machine in one office is too small. Two machines with failover, where you choose machines.

Who gets in. Your people sign in through your own single sign on, with roles for each team, so access follows the joiners and leavers you already manage.

What you can watch. The log goes to your own monitoring as well as staying on the system.

Recovery. The recovery point is the last nightly backup. The recovery time is measured on your system and written into the proposal, never quoted from a brochure.

03 What we answer for

Our mistake is never your person's.

Your person's yes covers what the screen showed them. The AI's work behind it is ours to answer for.

Nothing leaves until your person says yes.

They say it in two ways. Once, as rules: inside your prices, your limits and your hours, a reply goes at once. Or one at a time: anything outside those rules comes to their phone as one tap, ready to send.

If we stop, it is all still yours.

Every account is in your name from day one. Your files, rules and log come to you as plain files within 14 days.

When something goes wrong

AT ONCE

It stops

An agent that fails three times stops itself, and your team does that job the old way until it is fixed. At night and at weekends it stays stopped, and we pick it up at 09:00 on the next working day, unless your agreement includes weekend cover. You can stop any agent yourself, any time, in one tap.

BEFORE IT RUNS AGAIN

We fix it

The fix is proved on the case that failed and on twenty of your past jobs before the agent runs again. Fixing it is on us.

AT ONCE

You are told

Your own system tells your named person at once, at any hour, and Eashan writes to you with what happened and what we are doing about it. If your data is involved and we notice first, we tell your named person what we know within six hours of noticing, any day.

WITHIN FIVE WORKING DAYS

We write it down

A short review: what happened, why, what we changed, and what you need to do, which is usually nothing.

India's CERT-In directions give a company six hours from noticing an incident to report it. That is why the alert comes from your own system, at once, and never waits for a message from us.

04 Who works on your system

Who works on your system	Every person who works on your system is named in your proposal, with what each has built. Nobody else is given access to it.
Who signs, and who you escalate to	Eashan Gupta, founder. He signs the agreement and every note that needs an answer, and he is your escalation.
Support hours	09:00 to 19:00 India time, Monday to Friday. At night and at weekends your own system still stops a failing agent and tells your named person at once. Weekend cover is by arrangement, written into your agreement.
If we cannot be reached	Nothing unsafe waits on us. A failing agent stops itself, a working agent keeps working with your person approving, and you hold your own stop switch. Every account, file and log is already in your firm's name.

05 Our own AI policy

What our agents may do alone, how we test them and how we disclose. It binds the agents we run for you and the ones our own company runs on.

What an agent may do alone	Read, sort, draft, check and file, inside the rules its owner set. Those rules are written down, and a person can read them.
What always waits for a person	Spending money, signing, filing with an authority, deleting a record, and any message outside the rules its owner set.
How we test	Before an agent touches live work it runs on past jobs with known answers. Any change to its rules or its model runs the same jobs again first.

How we disclose

An agent that writes to a person outside the firm says it is AI at the start of every conversation. When one of ours gets something wrong, we say so in writing, as our error.

Your data

Your data trains only your own model, with your written yes, and never anyone else's. Nothing reaches another client. Where a model outside your own machine reads anything, it is named in writing before we build.

Who answers for it

A named person answers for every agent we run, ours and yours. The log shows what it read, what it did and who said yes.

06 What you own

- Every account and every line of code is in your company's name from day one.
- Your data, rules, prompts, templates and logs stay yours.
- The systems we build for you, and the machine if you choose one.
- If either of us stops, everything comes to you as plain files with a runbook, so another developer can run it.

The terms, in plain words

AI, said plainly

Agentec's AI drafts our notes and receipts and always says it is AI. An agent that speaks to people outside your firm says it is AI at the start of every conversation, in your firm's name.

The price, in writing

One fixed price, in writing, before any work. After the session you get a written proposal with the scope, the test it has to pass, who works on it and the price, and nothing starts without your yes.
agentec.cloud/engage

If you stop, or we do

Every account and every line of code is in your firm's name from day one. Your data, rules, prompts, templates and log come to you as plain files with a runbook any developer can use: at the end of the month you choose if you stop, within 14 days if we do. The machine in your office is yours.

Your files

Where they sit, what leaves the building and what is encrypted.
agentec.cloud/security

07 What is in writing first

Each of these is in your hands, in writing, before anything is built.

The scope, the plan and the price

In a written proposal, after the session and before you commit to anything: one fixed price, before any work.

Who works on your system

By name, with what each has built, and who may reach it for support.

Who else handles your data

With the machine in your office, nobody. In accounts in your firm's name, each provider is named, with what it reads.

What we answer for, and the exit

As this pack says it: the AI's work behind your person's yes is ours to answer for, and everything comes back to you as plain files if either of us stops.

Support and incidents

The support hours, what your own system does at night and at weekends, and when you hear from us.

Changes and reviews

How you ask for a change, and how it is tested on your own past jobs before it reaches live work. A note on what the system did and what changed, and a review each quarter.

08 The company, and who to write to

COMPANY

Agentec Intelligence Private Limited

CIN

U63999KA2026PTC225775

REGISTERED

Bengaluru, Karnataka, India. Incorporated on 10 August 2026.

GST

Registered in Karnataka since 23 September 2026.

DIRECTORS

As filed with the Registrar of Companies.

FOUNDER

Eashan Gupta, also chief technology officer of IKAN.

WRITE TO

hello@agentec.cloud

ONLINE

agentec.cloud/security

Send your questions, or your security questionnaire, to hello@agentec.cloud. A person reads every one and answers it. Every engagement is priced in writing after the session, one fixed price before any work, and this pack comes with the proposal.

Agentec Intelligence Private Limited. CIN U63999KA2026PTC225775. agentec.cloud