



SECURITY OVERVIEW

How we protect your data, your systems and your intellectual property on every engagement.

Written for the security, legal and procurement teams reviewing TriadKube as a technology partner. It sets out the practices we apply by default, from the first conversation to the last day of handover.

Version 1.0 · September 2026 · triadkube.com/security

At a glance

- ✓ Confidentiality is agreed before we see any of your systems, data or documents.
- ✓ Your data stays in the region you choose and is encrypted in transit and at rest.
- ✓ Named accounts, multi-factor sign-in and least-privilege access, all revoked at handover.
- ✓ Every change is peer reviewed and scanned for vulnerabilities before it reaches production.
- ✓ You own the code, the infrastructure and the documentation from the first commit.

OUR POSITION

Why security is settled before the work starts

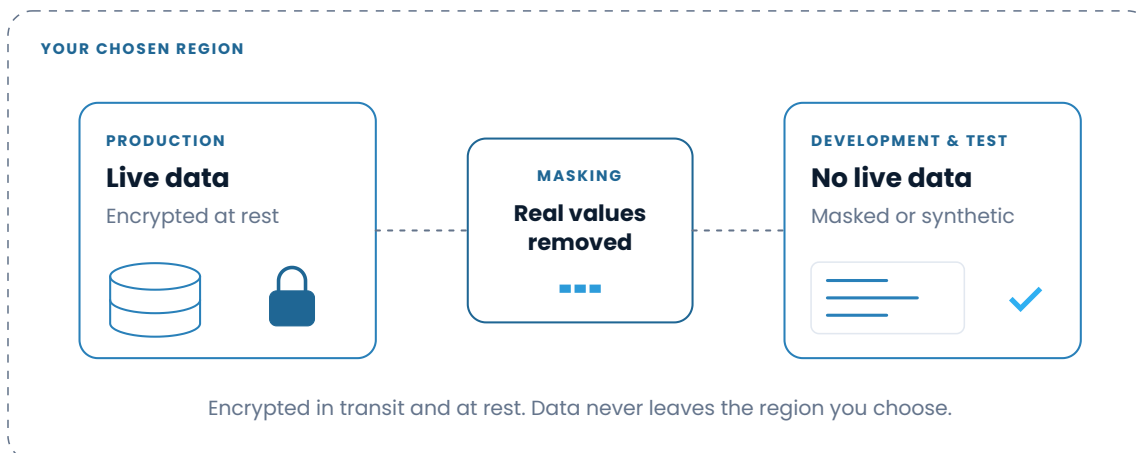
Giving a partner access to your systems is a risk decision before it's a technical one.

Your security team needs to know where the data will go, who can reach it, what happens to it at the end, and what record will exist if an auditor, a regulator or your own board asks. We answer those questions before the first login is created. The practices in this document apply to every engagement by default, they're written into the agreement, and each one leaves a record your team can inspect.

Security isn't a phase of our work. It's the condition every phase runs under.

How we handle your data, and where it lives

Data handling is agreed before any access is granted: what data the work needs, where it will be stored and processed, and who can reach it. We ask only for the data the work requires.



Your environment first

If you provide an environment, we work inside it, under your policies and your monitoring. If you don't, the work runs on TriadKube's secured cloud infrastructure, and production is set up in accounts your organization owns.

Live data stays in production

Development and test environments never hold production data. Where realistic data is needed, we use masked or synthetic data.

Your region, and only your region

Your data stays in the region you choose. We don't copy it to another location or into tools outside the agreed environment. Our engineers work on it where it lives.

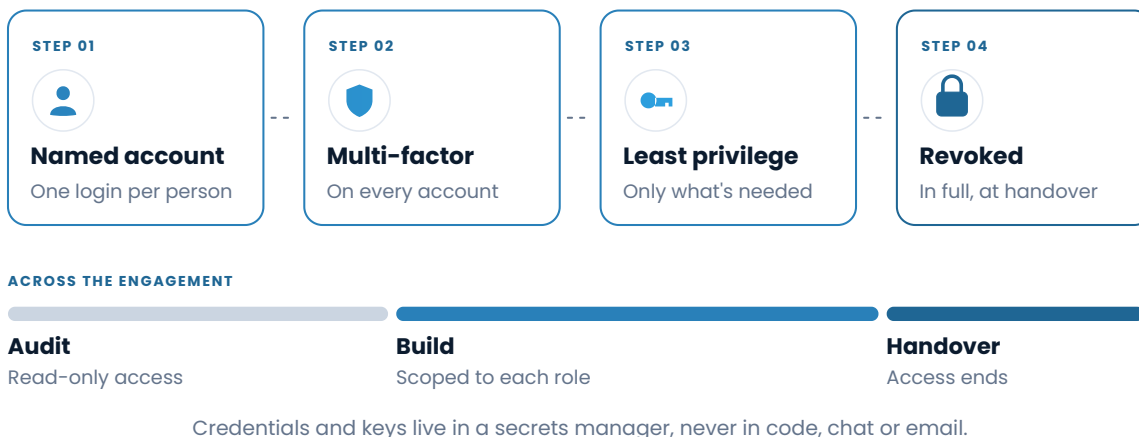
Encrypted in transit and at rest

Data is encrypted whenever it moves between systems and wherever it's stored, in every environment we build or operate for you.

02 · ACCESS CONTROL

Who can access your systems, and for how long

Only named people, only with the access their role needs, and only while the engagement runs.



- ✓ Every person has an individual, named account. There are no shared logins.
- ✓ Every account is protected by multi-factor sign-in.
- ✓ Access is scoped to each role and to the systems in scope. The architecture audit runs on read-only access.
- ✓ Credentials, keys and tokens are held in a secrets manager, never in code, chat or email.
- ✓ At handover, credentials pass to your team and every TriadKube account is revoked.

03 · INTELLECTUAL PROPERTY AND CONFIDENTIALITY

Who owns what we build

You do. Confidentiality is agreed before we see anything, and ownership is written into the contract rather than left to interpretation.

Confidentiality first

A non-disclosure agreement is in place before we see your systems, data or documents, with terms agreed for your engagement.

Your repositories from day one

Source code lives in repositories under your organization's account from the first commit.

Ownership in the contract

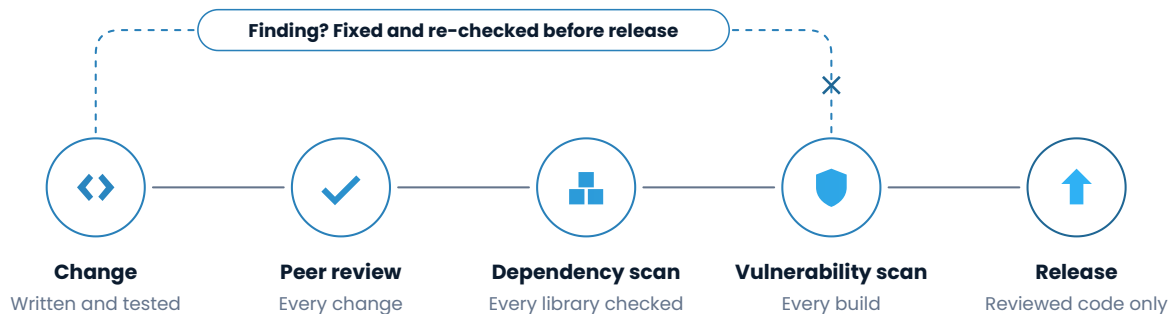
The master services agreement assigns ownership of the code, configuration and documentation we produce to you.

Your accounts, your name

Production infrastructure is set up in accounts your organization owns, so nothing you depend on sits in ours.

How security is built into the code we write

Security is checked on every change, not tested once at the end. Nothing reaches production until it has passed each of these steps.



Development, test and production kept separate. Credentials never stored in code.

01 Security in the design

The architecture audit assesses security alongside your applications, integrations and data flows, and the target architecture addresses each risk it finds before build starts.

02 Peer review on every change

No change is merged without review by a second engineer. Reviews look at how the change handles data and access, not only at whether it works.

03 Automated scanning before release

Every build is scanned for known vulnerabilities in our code and in the third-party libraries it depends on. Findings are fixed and re-checked before release.

04 Separated environments

Development, test and production are kept apart. Production data lives only in production, and production access is limited to the people who release to it.

The record you keep of what we did

Every decision and every change leaves a written trail that stays with your team after we've gone.

- ✓ Every code change is linked to its review: who changed what, when, and who approved it.
- ✓ Architecture decisions are recorded with the reasoning behind them and the options considered.
- ✓ Progress, risks and decisions are reported in writing at a cadence agreed at kickoff.
- ✓ Scope changes go through a documented process, with their impact assessed before approval.
- ✓ Each phase closes with a written sign-off from your stakeholders.
- ✓ A record of who held access, to which systems, and when it was revoked is handed over with the project.

Who else will have access to your data

No one you haven't approved.

Our own team does the work

Every engagement is staffed with at least five TriadKube people, and you meet them before the work begins.

Specialists join on the same terms

When a vetted specialist is needed, you're told before they start. They're bound by the same confidentiality terms and follow the same access rules as our own engineers.

No service sees your data without your approval

Any third-party service that would store or process your data is named to you and approved by you before it's used. Where you'd rather we use your own tools, we work in them.

COMMON QUESTIONS

Questions a vendor review usually asks

Will you complete our vendor security questionnaire?

Yes. Send it with your first enquiry or at any point during evaluation. A senior architect completes it, and the answers match this document and triadkube.com/security.

Can you work under our own security policies?

Yes, and we prefer to. Where you provide the environment, we work inside it under your access, device and change policies, and your team keeps its own monitoring over everything we do.

What happens to our data when the engagement ends?

Credentials pass to your team and every TriadKube account is revoked. Any of your data held on TriadKube infrastructure is returned or deleted as your agreement specifies, and we confirm in writing when it's done.

How do you handle cross-border engagements?

TriadKube works with clients in India, Germany and the USA. Your data stays in the region you choose, and our engineers work on it there through named, multi-factor accounts rather than moving it to where they sit.

Take any part of this further with a senior architect.

We'll walk your security, legal or procurement team through any section of this document in a technical session.

hello@triadkube.com · triadkube.com/security

This overview describes the practices TriadKube applies on every engagement. Contractual terms, including confidentiality, ownership and data handling at the end of an engagement, are set out in the non-disclosure agreement and master services agreement agreed with each client.