SOVEREIGN AI

Powerful AI. On your terms.

Private by default. Verifiable in operation. Built to keep you in control.

Put AI to work with your information, your systems, and your people. amotivv brings together private infrastructure, capable models, and accountable operation in a service your organization can understand and approve.

OUR GROUNDING

Built by people who operate critical systems.

Our background in infrastructure, telecommunications, and data shapes how we build AI. We look beyond the model to the systems it depends on: access, capacity, security, continuity, and recovery. As technology changes, that operating discipline gives customers a dependable foundation for adopting new capabilities.

01 **Collapse dependencies.**

Bring processing into controlled environments instead of passing information through unnecessary providers. Reduce exposure to their changing terms, technology, and security posture.

02 **Maintain capability.**

Combine self-hosted intelligence, connected tools, and approved frontier models. Choose the right capability for the work, within the organization's data and access requirements.

03 **Preserve control.**

Keep models, software, operating knowledge, and evidence portable. Changes in infrastructure must preserve customer protections rather than force acceptance of weaker terms.

Own the capability. Keep the freedom to evolve.

Sovereignty is practical control over how AI works for your business, without having to build and maintain the entire stack yourself.

ONE ACCOUNTABLE OPERATING TEAM

Private AI. Complete service.

Infrastructure, models, access controls, and evidence, integrated around the work your business needs to do.

THE CONTROLLED PROCESSING PATH

Authority · Execution · Evidence

Your information and systems
Authorized sources
Scoped access

→

Private AI environment
Protected processing
Attested environment

→

Useful results and evidence
Analysis and actions
Inspectable records

Approved frontier access Additional intelligence participates through explicit permissions and data boundaries.

01 / CONFIDENTIALITY

Protect data while it works.

Confidential computing protects data during processing. Private networking and identity-based permissions control access to connected systems.

02 / VERIFIABILITY

Inspect the protections.

Hardware-backed attestation verifies the environment. Signed authorization and evidence records make the recorded work independently checkable.

03 / US RESIDENCY

Know where work happens.

Physical US placement is an explicit requirement. Defined locations and data boundaries give security and legal teams a concrete deployment to assess.

04 / OPERATING CONTROL

Manage change deliberately.

Self-hosted models and dedicated capacity put versions, updates, resource allocation, and cost planning under our management.

05 / PORTABILITY

Keep the ability to move.

Deployable models, software, state, and evidence preserve options across hosts. Customer protections govern every infrastructure transition.

06 / ACCOUNTABILITY

Put the operating work with us.

We manage integration, dependencies, security changes, and recovery. Your team focuses on business outcomes rather than maintaining the infrastructure.

Put private AI to work.

Start with one valuable workflow. Define its information boundaries, operating requirements, and measurable outcome.