

FORCE

12 NON-NEGOTIABLE REQUIREMENTS



Enterprise AI Sovereignty

If the provider cannot satisfy all five FORCE pillars and the twelve requirements below, treat the failure as the risk assessment—not a negotiation inconvenience.

F	O	R	C	E
Fiduciary Custody	Operational Continuity	Resilience Against Monoculture	Control & Organizational Autonomy	Egress & Exit

1. Defined Ownership and Control of Enterprise-Created State Define ownership, control, export, reuse, retention, and deletion rights for every customer-created or customer-funded state.	7. Resilience Against Monoculture and Single-Provider Failure Avoid critical dependence on one provider, model family, cloud, identity plane, alignment policy, or inference path.
2. No Secondary Use Without Explicit Authorization No training, model improvement, benchmarking, advertising, product development, or unrelated human review without specific, revocable permission.	8. Least Privilege and Customer-Controlled System Boundaries Limit data, tools, credentials, network paths, code execution, and authority to the approved task.
3. Sovereign Custody and Cryptographic Control Control must be physical, operational, jurisdictional, and cryptographic—not data residency alone.	9. Independent Audit, Incident Disclosure, and Evidence Preservation Preserve logs, model identifiers, instructions, state, permissions, and incident evidence for customer and independent review.
4. Model Version Pinning and Validated Baselines A validated model performing consequential work must not be silently replaced by a materially different model.	10. Nondelegable Responsibility and Contractual Liability Allocation “The AI acted autonomously” must not operate as a blanket defense against negligent design, permissions, monitoring, integration, or deployment.
5. Governed Change, Notice, Testing, and Rollback Material behavior, policy, alignment, capability, and safety changes require notice, testing, evidence, transition, and rollback.	11. Complete Cognitive Export and Functional Migration Export must support meaningful reconstruction of context, memory, workflows, configurations, and capability in another environment.
6. Retirement, Service Continuity, and Provider-Failure Protection Maintain a tested continuity path if a model, service, provider, subprocessor, or contract ends.	12. No Punitive Exit and a Tested Exit Capability Exit must be economically, technically, and operationally real—and proven before dependence becomes irreversible.

THREE BOARD GATES: Who controls the intelligence? | Can we keep operating? | Can we leave?

Board test: Can you inspect it, preserve it, move it, and operate without it? If not, you have an unmanaged dependency.	NO FORCE. NO DEAL.
--	-------------------------------