



Policy paper — AI sovereignty as enabling conditions

© John Stroh

Version 0.1 · revised 4 September 2026 · [this version as a PDF](#)

Drafted with AI assistance, then checked and revised by the author. The judgements and the errors are the author's.

Draft paper for consideration by the Board of The Opportunities Party

1. The ask

That the Party adopt AI sovereignty as a platform position, expressed as **enabling conditions** rather than as a programme, an agency, or an investment.

Nine proposals follow. Five cost nothing. Two are procurement commitments rather than appropriations. None of them names a provider, establishes an entity, or requires any particular organisation to exist.

That neutrality is deliberate and it is the point. Conditions can be adopted by this Party and later by others. A vehicle can only ever belong to whoever established it.

2. The problem, briefly

FIG-09 NOBODY PROCURED THIS

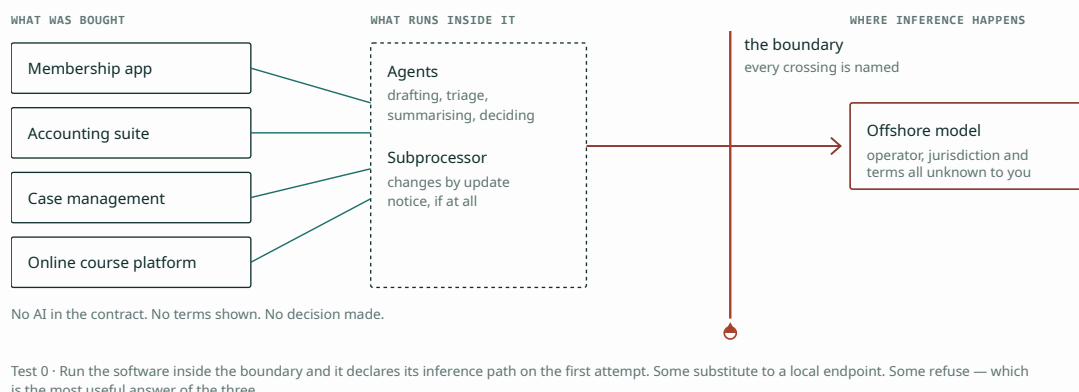


FIG-09 AI now arrives as a property of software already bought. The boundary is how a member finds out: run it inside, and it declares its inference path on the first attempt.

The public argument is about whether New Zealand has an AI strategy. It is the wrong question, and answering it produces work programmes rather than protections.

The right question is whether an organisation here — a small business, a professional practice, a school, a trust, a community group, a council, a university, an iwi entity — can do five things without becoming permanently captive to a foreign platform. Most of the organisations affected are small: they have no procurement function, no legal budget, and no way to read a subprocessor notice even if one arrived.

1. Store and govern sensitive data under an appropriate jurisdiction.
2. Access affordable compute for legitimate public-purpose work.
3. Build or deploy a model, or use an application, without surrendering data for vendor training.
4. Move data, applications and workflows to another provider at will.
5. Refuse a vendor's terms without losing the ability to govern.

Assessed against the Sovereignty Assessment Instrument (published separately, vendor-neutral, applicable by anyone), New Zealand currently fails tests 1, 4 and 5 and partially satisfies 2 and 3. **We have adoption. We do not have sovereignty.**

On urgency. The dependency risk is generally assumed to be American. The medium-term trajectory is at least as likely to run the other way, because the open-weights ecosystem available as a fallback is substantially maintained in China. In this sector a pivot takes weeks. A country discovers it is captive at the point where the discovery no longer helps.

3. Why the existing instruments do not answer it

New Zealand has a July 2024 Cabinet paper on the approach to AI, which reasons that existing law provides guardrails and that a standalone AI Act is not preferred. It has an AI Strategy from MBIE (July 2025) which deliberately emphasises adoption and application over foundational development. It has a Public Service AI Framework led by the Government Chief Digital Officer.

All three are deliberately light-touch. None binds. There is no AI-specific legislation and none has been tabled.

This paper does not propose replacing them. It proposes adding enforcement to instruments that already exist.

4. Proposals

FIG-01 THE SIX TESTS · AOTEAROA NEW ZEALAND · AUGUST 2026

00	Discovery	FAIL
Can the organisation find out whether it is using AI at all?		
01	Jurisdiction	FAIL
Data located here AND operator beyond foreign compulsion		
02	Compute	PARTIAL
Affordable compute for public-purpose work, outside the research system		
03	Non-extraction	PARTIAL
Protection that is verifiable, and survives a change of terms		
04	Portability	FAIL
Complete operational state moves, with a measured time		
05	Refusal	FAIL
Decline a unilateral change of terms and still discharge statutory functions		
Overall		
FAIL		
The finding is the lowest score, not the average. Sovereignty is not a portfolio.		

FIG-01 Six tests for whether a country has AI sovereignty or only AI adoption, beginning with whether it can tell. New Zealand's current position, with each verdict against its own row. The finding is the lowest score, not the average.

4.0 Require an inference-path declaration in the software supply chain (low cost)

Any software product supplied to a public body declares whether it performs inference, which models are used, operated by whom, in which jurisdiction, under what data terms — and notifies the buyer on material change.

Why this comes first. Every other proposal in this paper assumes an organisation knows it is procuring AI. Most no longer do. AI now arrives as a property of software already bought, changed by subprocessor update, never surfaced at the point of sale. An agency cannot

govern, refuse or assess what it cannot see.

Why it is achievable. This is a bill of materials extended from security to the inference path. The security equivalent moved from novel to procurement-standard within a few years. The argument to officials is not “regulate AI” — it is “you already require disclosure of software components for security reasons; extend the schedule.”

Where a vendor will not disclose, that refusal is the disclosure, and is more useful to the buyer than a blank.

4.1 Define the sovereignty test in procurement (*no cost*)

Adopt a two-part definition of sovereign infrastructure for public procurement: data physically located in New Zealand, **and** the operating entity beyond foreign legal compulsion — no foreign parent, no foreign controlling shareholder, no foreign assets exposed to seizure, no supplier obligation to disclose on foreign demand.

Data location and jurisdiction are not the same property. A hyperscaler region in Auckland satisfies the first and fails the second, and is widely sold as though it satisfied both.

4.2 Define “suitable onshore service exists” (*no cost*)

Cloud First provides that RESTRICTED information should, over time, be stored in a New Zealand-based data centre **where a suitable onshore service exists**. The term is not authoritatively defined. On a location-only reading, the arrival of hyperscaler regions satisfies it and the clause expires quietly.

Defining suitability by 4.1 converts a dormant sentence into the strongest sovereignty provision in New Zealand procurement. The sentence is already there. It costs nothing to enact and changes the most.

4.3 Make jurisdictional risk binding (*no cost*)

Cloud Jurisdictional Risk guidance was updated in 2024 and supports agencies’ case-by-case risk assessments. It advises; it does not bind.

Make operator compulsion a mandatory and evidenced element of the assessment, such that an assessment considering only data location is non-compliant. The instrument exists and has an owner. This is a change of status, not a new work programme.

4.4 Exempt sovereignty-qualifying infrastructure from the on-premise restriction (*no cost*)

Public service agencies and some Crown entities may not invest in on-premise ICT infrastructure unless specified criteria are met or the GCDO approves.

That rule was framed before capable models could run on hardware available at retail. It now operates as a barrier to agency-controlled or community-controlled compute. Infrastructure meeting the 4.1 test should not be treated as on-premise investment for the purposes of the restriction.

4.5 Statutory protection against public-sector data entering vendor training (*low cost*)

A prohibition, not a disclosure regime, with an audit right, a notification obligation on change of terms, and a penalty.

The rationale is the irreversibility of training. Data used to train a model cannot be withdrawn from it. Where harm cannot be undone, remedies after the fact are decoration and only an *ex ante* constraint does any work. This is the single strongest argument available for regulation in this area and it is not contested by anyone technical.

Note that the required terms are already commercially available; the gap is that they are vendor-written, vendor-variable, unverifiable by the customer and subordinate to foreign legal process. Legislation converts a purchasable assurance into an enforceable right.

4.6 Crown anchor tenancy, open to any qualifying operator (*procurement, not appropriation*)

Rather than capitalising providers, commit to multi-year service offtake at defined volumes, available to any operator meeting the 4.1 test.

Committed revenue is more bankable than a grant, survives a change of government better than a line item, requires no novel structure, and — critically — does not put the Crown into the governance of the entities it buys from. It also flips the proposition from *fund this* to *buy this*, which is a conversation officials already know how to have.

4.7 Give effect to commitments already made (*no cost*)

Cloud First already requires agencies to consider te ao Māori perspectives for Māori data, with guidance in development through Internal Affairs, Statistics New Zealand and the Data Iwi Leaders Group. It already requires a multi-cloud approach avoiding over-dependence on any specific supplier.

Both are stated. Neither is enforced against the dependency that matters. Government is not being asked to adopt a new principle — it is being asked to make two of its own operational, and to complete the Māori data guidance rather than leave it in development.

A note on scope. Nothing in this paper resolves who holds authority over iwi and whānau data when processing occurs offshore. Everything above is jurisdictional. That question is prior to jurisdiction and should be answered with, not for, Māori data governance leadership.

4.8 Establish a sovereign timestamp authority (*modest, and time-limited*)

Establish a New Zealand timestamp authority under an existing records mandate, with a published algorithm-renewal policy and recognised evidentiary standing in New Zealand law.

The problem is already named by government. The New Zealand Information Security Manual has carried post-quantum guidance since January 2022, directing agencies to inventory cryptographically protected assets and plan migration. Version 3.9 records that quantum developments can undermine all widely used public key algorithms for digital signatures, that quantum-resistant replacements will be needed in the near future, and — the sentence that matters here — that historical and archived data may be at risk.

The gap is specific and no agency can close it alone. Migration guidance protects records written from now on. It does nothing for records already signed, which do not merely become insecure: they become **retroactively forgeable**. At that point a classical signature proves nothing about what a record said or when it was written.

What survives that transition is an independent timestamp — proof that a record existed in a particular form at a particular time, anchored to a party with no interest in the record and renewed under fresh algorithms before the old ones weaken. An agency timestamping its own records proves nothing to anybody else. This is shared infrastructure by definition, which is why it has no owner and why it will not appear unless someone is asked to build it.

Why now rather than next term. The records at risk are the ones being written today. This cannot be retrofitted, because retrofitting means re-signing history nobody controls any more. It is the same shape as the irreversibility argument at 4.5: a delay is not a deferral, it is a permanent loss of the records created during the delay, and nothing announces the moment it becomes too late.

Where it might sit, and why one candidate stands out. Archives New Zealand holds the Public Records Act mandate for the digital record of government. Its Archives 2057 strategy already anticipates that not all records of enduring value will be transferred to the archive, and that technology will provide methods of assuring authenticity and trustworthiness of records whether archived or in current use.

Assuring the authenticity of a record held by someone else is exactly what an independent timestamp authority does. The strategy names the requirement; nothing published names the mechanism. GCSB holds the cryptographic standards role and DIA the digital mandate, so the right home is a question for the three of them — but an existing mandate can be extended rather than a new institution created.

One dependency to resolve alongside it. A timestamp is only useful if a New Zealand court will accept it. Establishing the authority without evidentiary standing produces a service nobody is obliged to rely on, so the legislative work and the operational work should proceed together.

Scale. A timestamp authority is not a data centre and not an AI programme. It receives hashes and returns signed tokens. The hard parts are institutional rather than technical — key custody, a renewal policy, continuity of the operator across decades, and standing in evidence.

Declared interest. The author would like to help design this and could prototype the requirement. He is structurally disqualified from operating it, and says so: a timestamp authority derives its entire value from independence of the parties relying on it.

5. What this paper does not propose

- No new agency, regulator or institute.
- No named provider, and no entity established by the Party.
- No data centre subsidy or national megaproject. The premise that sovereign compute requires hyperscale is out of date.
- No prohibition on the use of foreign AI services. The proposal is that refusal remains possible, not that adoption is prevented.

6. Costings

PROPOSAL	COST
4.0 Inference-path declaration	Schedule change to procurement terms; low
4.1 Define sovereignty test	Nil — definitional
4.2 Define suitable onshore service	Nil — definitional
4.3 Binding jurisdictional risk	Nil — status change to existing guidance
4.4 On-premise exemption	Nil — may reduce cost by permitting cheaper options
4.5 Statutory training protection	Drafting and enforcement capacity; modest
4.6 Anchor tenancy	Procurement of services agencies would otherwise buy elsewhere
4.8 Sovereign timestamp authority	Modest establishment and ongoing operation; smaller than any other item here
4.7 Give effect to existing commitments	Nil to complete guidance already in development

7. Sequence

FIG-07 THREE AMENDMENTS TO INSTRUMENTS ALREADY IN FORCE

IN FORCE TODAY	AMENDED	COST
"...where a suitable onshore service exists" undefined; a region satisfies it	→ Suitability defined by the two-part sovereignty test	nil
Cloud Jurisdictional Risk guidance (2024) advisory to a risk assessment	→ Operator compulsion becomes a mandatory, evidenced element	nil
No on-premise investment without GCDO approval	→ Sovereignty-qualifying infrastructure is not on-premise investment	nil

FIG-07 Three changes to instruments already in force. Five of the seven policy proposals cost nothing; these three cost nothing and need no legislation.

Immediate, requiring no legislation: 4.2, 4.3, 4.4 — all achievable by Cabinet decision or ministerial direction within existing instruments.

Next: 4.1 as a procurement standard, 4.6 as a procurement commitment.

Legislative: 4.5, and any statutory footing for 4.7.

8. Anticipated objections

“This is protectionism.” It sets a test any operator may meet, including foreign-owned operators willing to restructure. It excludes nobody by nationality and everybody by structure.

“It will raise costs.” Possibly, at the margin. The comparison is not with today’s price but with the price after a vendor has become unrefusable. That is what the fifth test measures.

“Government should build the capability.” Sovereignty achieved by dependence on the Crown is re-domiciled dependence. Anchor tenancy achieves the outcome without placing the Crown in the governance of the entities it depends on.

“Nobody can meet this test anyway.” Foreign silicon, firmware and driver stacks are universal and no provider on earth escapes them. The test is scoped to the operator and the data path for that reason, and that scope limit should be stated openly wherever the test is applied.

9. The opening

As at early August 2026, the only party to have released AI policy for this election is the Greens, with a proposed one-year moratorium on new data centre consents. Commentary from within the sector has noted that New Zealand’s trading partners have all adopted some

form of AI rules and that appearing out of step is itself a soft-power cost.

The field is open. No party currently holds the position that New Zealand should be able to use this technology without being owned by it.

Sources: digital.govt.nz Cloud First policy and Cloud Jurisdictional Risk guidance; All-of-Government Cloud Sourcing Strategy; MBIE AI Strategy July 2025; Cabinet paper July 2024; MBIE/Beehive material on the NZIAT AI Research Platform; published vendor enterprise privacy terms; contemporary sector commentary. Retrieved 20 August 2026 — verify before publication.

►DISCLAIMER

Cite this version

Policy paper – AI sovereignty as enabling conditions, version 0.1 (September 2026). agenticgovernance.digital/downloads/enabling-conditions-v0-1.pdf

Licensed CC BY 4.0. Reuse is free, including commercially, provided the author is credited and the reuse does not suggest that the author endorses it. This link is frozen at version 0.1; [/enabling-conditions](#) always shows the current one.

PREVIOUS

G · Why records signed today may not survive

Series contents

NEXT

I · What actually stops an AI doing the wrong thing

Alongside: [slides](#)