Governance That Can’t Be Quietly Undone

Tamper-evident community and kāhui Māori governance — and the AI rules of Aotearoa New Zealand and Australia

John Stroh · Director, My Digital Sovereignty Ltd
Research: agenticgovernance.digital

Full essay: agenticgovernance.digital/papers/tamper-evident-governance.html

The rules are softer than they look

Neither country has passed prescriptive AI legislation.

- **NZ:** National AI Strategy + Public Service AI Framework (July 2025) — *"not binding"*; the **voluntary** Algorithm Charter; the **Privacy Act 2020** (the one hard anchor).
- **Australia:** 10 mandatory guardrails **proposed Sept 2024** — then **shelved by the Dec 2025 National AI Plan** for existing tech-neutral law + the Voluntary AI Safety Standard.
- Expectations are real and converging (OECD-aligned); **enforcement is mostly good faith and self-report.**
- **Adjacent law is moving fast:** Privacy Act amended (IPP 3A, May 2026); **Crimes (Countering Foreign Interference) Amendment Act 2025** (in force Nov 2025) — integrity & national-security context, *not* AI regulation.

→ NZ Public Service AI Framework · AU National AI Plan trajectory

What good governance is actually asked for

The same expectations recur on both sides of the Tasman:

- **Transparency** — disclose when and how AI is used.
- **Human oversight & accountability** — a named human decides the consequential things.
- **Record-keeping & auditability** — decisions traceable, reviewable, independently checkable.
- **Fairness & contestability** — those affected can understand and challenge a decision.
- **Privacy & data protection** — Privacy Acts; in Aotearoa, **Te Tiriti** for Māori data.
- **Risk-proportionality** — heavier scrutiny where stakes are higher.

Make the principle structural

Move the load-bearing commitments out of policy and into architecture.

- Where a **policy can drift**, a **proof chain cannot be silently rewritten**.
- Where a **promise can lapse**, a **constitutional floor holds**.
- Where an **operator could be compelled**, one that **cannot read the data cannot disclose it**.

In a regime that chose principles over hard law, the differentiator between real governance and governance theatre is whether the principles are enforced where they cannot quietly be undone.

Tamper-evident by construction

- **Sovereign records** — every record carries embedded origin, policy, and a **signed, append-only proof chain** (per-tenant Ed25519 keys); external `$pull` / `$set` rejected in the data layer. A decision's history reconstructs from the community's own data, without trusting the operator.
- **A constitutional floor** — `BoundaryEnforcer` keeps the AI presenting options, never making value/governance decisions; above it a universal rule layer *"cannot be overridden by any tenant configuration."*
- **Deterministic guardians** — rules + thresholds, not learned models: reproducible, auditable; closer to rule-checkers than the probabilistic systems AI regulation targets.
- **Audit native** — `GovernanceAuditLog` records rules checked, outcome, time; rule changes logged before/after.

"Tamper-evident," not court-proof — signed with the tenant's own keys (the platform names the limit).

Data sovereignty, mechanically

- Hosting **EU/NZ only** (OVH France, Catalyst NZ); inference run **locally**; zero US data-processing footprint.
- **Per-record encryption**; **cryptographic deletion** destroys the key — unrecoverable even by the operator — and leaves a **signed tombstone** (erasure *evidenced*, not erased-without-trace).
- Every query **tenant-filtered**: an operator served a foreign order *"cannot disclose what they cannot read."*
- The Privacy Act’s cross-border concern, and **Te Tiriti’s** data-sovereignty concern, answered mechanically.

How a governance village runs

- **A constitution first** — sovereign sections (conflict-resolution, values, federation posture) **hard-gated** before any content.
- **Deliberation as a signed record**; closure leaves a signed entry naming the decision, date, and policy.
- **Voting** — attributed / anonymous / roll-call; **quorum locked to a membership snapshot at poll-open** (immutable — mid-vote changes can’t move it).
- **A governance queue with deadlines** — create → acknowledge → decide → enact (or reject).
- **Authority plural and withdrawable**; **committee + governance demos live**.
- *In development:* full signed minutes export, motion-sequencing enforcement, conflict-of-interest prompts.

Kāhui Māori villages

Scaffolding for Māori-led governance — not the platform speaking for anyone.

- **Whakapapa held as taonga** (Te Tiriti Art. 2): mandatory **kaitiaki attribution** + the **tikanga under which shared**.
- **Disclosure governed by tikanga**, not platform policy — whānau-only … hapū … kaitiaki-only … never-shared; refused at the read boundary.
- **Cross-iwi sharing is bilateral only**, by bilateral federation agreement, fully revocable — no central register, no Crown-mediated graph.
- **Operator structurally cannot read across iwi**; te reo in the vocabulary system; training data under **Taiuru's Kaupapa Māori AI Framework**.
- **Kāhui Māori demo live**; production iwi-to-iwi federation awaits a counterparty agreement — *a decision for iwi.*

The limits, stated plainly

- *In development:* full signed minutes export, strict motion-amendment sequencing, conflict-of-interest recusal, formal constitutional-amendment workflow, vote revocation.
- Te Tiriti compliance position **published for feedback (v0.2)**; formal legal opinion still to come.
- Post-quantum crypto and hardware-backed keys are **roadmap**.
- **"Tamper-evident," not court-proof** — tenant-key signatures, not a third-party notarised timestamp.
- None of it undercuts the core claim.

The rules may be soft. The governance need not be.

Aotearoa and Australia ask communities and agencies to be **transparent, accountable, auditable, and respectful of data sovereignty.**

The platform's answer is to make those properties of the **architecture** — so meeting the rules is the **default behaviour** of the system the community already runs on, not a quarterly attestation.

> Where a policy can drift, a proof chain cannot be silently rewritten; where an operator could be compelled, one that cannot read the data cannot disclose it.

Full essay: agenticgovernance.digital/papers/tamper-evident-governance.html · CC BY 4.0