



A KEYTECH INTELLIGENCE PERSPECTIVE ON  
DATA, AI AND TRUST

# Sovereign by Design.

Where your data lives, whose laws it answers to, and why that question now shapes every AI decision an Australian organisation makes.

A guide for business leaders, boards and community organisations.

YOUR DATA.  
OUR **OBSESSION.**

# Inside this guide

|    |                                         |
|----|-----------------------------------------|
| 03 | A word from our founders                |
| 04 | Why we chose Macquarie                  |
| 05 | Residency, sovereignty and localisation |
| 06 | Why sovereignty matters now             |
| 07 | What makes a data centre sovereign      |
| 08 | Five reasons to host sovereign          |
| 09 | Does your organisation need it?         |
| 10 | Sovereign AI explained                  |
| 11 | What sovereign AI requires              |
| 12 | Sovereign AI around the world           |
| 13 | How we build: a view from our CTO       |
| 14 | From Essential Eight to Essentials      |
| 15 | Launch AI by Macquarie                  |
| 16 | Private cloud and private connectivity  |
| 17 | Assess your data position               |
| 18 | How Keytech can help                    |
| 19 | Onboarding into Keytech Core            |

Data sovereignty is not an IT setting. It is a business decision about trust, risk and accountability, and it belongs on the agenda of every leadership team.

# A word from our founders

Luke Lispet, Chief Executive Officer · Shaune Irving, Chief Technical Officer



Luke Lispet and Shaune Irving, founders of Keytech Intelligence.

We started Keytech Intelligence with a simple conviction: Australian organisations deserve technology they can trust, built by people who understand what is at stake when information falls into the wrong hands.

Artificial intelligence is changing how every business works. It is also changing the stakes. The documents, conversations and records that feed an AI system are among the most valuable things an organisation owns. Yet many leaders still cannot say with confidence where that data is stored, which laws apply to it, or who could be compelled to hand it over.

We are proudly an Australian owned and veteran owned private enterprise. Our backgrounds in service shaped how we think about trust, duty and protecting what matters, and that is how we build for our clients. We answer to the organisations we serve and to Australian law, with no foreign parent and no outside agenda.

This guide brings together what we have learned building secure platforms for high-risk environments. It explains data sovereignty in plain language, looks at the rise of sovereign AI, and gives you practical questions to test your own position.

Our hope is simple. Read it, share it with your board, and take a serious look at where your data sits today.

# Why we chose Macquarie

Luke Lispet, Chief Executive Officer

When we designed our platforms, the first decision was not which features to build. It was where our clients' information would live, and under whose rules. We concluded early that the answer had to be Australian infrastructure, operated under Australian law.

That is why Keytech Intelligence works in partnership with **Macquarie Technology Group** and **Macquarie Cloud Services**. Macquarie is Australian owned and operated, part of the ASX-listed Macquarie Technology Group, and has been building and running data centres in Australia for more than 20 years. Its facilities are among the few certified at the Strategic level under the Australian Government's Hosting Certification Framework, and it is trusted with sensitive data by a large share of Commonwealth government entities.

Through Macquarie Cloud Services, our platforms run on Australian Managed Azure. Our clients get the capability of the Microsoft ecosystem with their data kept onshore, managed by an Australian provider, and backed by infrastructure certifications held by Macquarie, including ISO/IEC 27001 and IRAP assessment at PROTECTED.

## INFRASTRUCTURE

### Macquarie Technology Group

Australian-owned data centres certified at the Strategic level for government hosting.

## CLOUD

### Macquarie Cloud Services

Australian Managed Azure, keeping workloads onshore under Australian management.

## PLATFORM

### Keytech Intelligence

Secure, sovereign-by-design platforms and AI systems built on that foundation.

## OUTCOME

### For our clients

Capability without compromise: modern AI, with data that stays answerable to Australian law.

## OUR TRUSTED TECHNOLOGY PARTNER



Partnership with Macquarie is not a logo on a slide. It is the foundation that lets us make a promise to our clients and keep it.

# Residency, sovereignty and localisation

Three terms are often used as if they mean the same thing. They do not, and the difference matters when you sign a contract with a technology provider.

## WHERE

### Data residency

The physical location of your data, for example a data centre in Sydney. Residency alone does not stop data being subject to foreign laws, transferred offshore or accessed from overseas.

## WHOSE RULES

### Data sovereignty

The laws your data is subject to because of where it sits and who controls it. Sovereign data answers to Australian law, and Australian law alone.

## HOW STRICT

### Data localisation

A stricter form of residency: data generated in a country must be stored and processed there before it can be used elsewhere.

## WHAT MATTERS

### Processing, not just storage

It is not only where data is stored. It is where it is processed, who operates the systems, and who could be compelled to provide access.

If residency is where the game is played, sovereignty sets the rules of play.

A provider can truthfully say your data is stored in Australia while the company controlling it remains subject to the laws of another country. True sovereignty requires onshore infrastructure, Australian control and Australian jurisdiction together.

Onshore is a location. Sovereign is a commitment.

# Why sovereignty matters now

Our world runs on connected data. That connection drives collaboration and innovation, but it raises hard questions. When information flows freely across borders, who controls it, and how do we know it is protected?

## SECURITY

### Fewer weak points

Data held under Australia's security and privacy laws reduces the gaps that cybercriminals exploit, and the risk to critical services.

## PRIVACY

### Control stays local

Personal and financial records remain on Australian shores, shielding customers from misuse and reducing legal risk for the business.

## A changing landscape

Australia has seen a sharp rise in cybercrime in recent years, including some of the largest breaches of personal health and government information in the nation's history. Government has responded:

- the **Whole-of-Government Hosting Strategy** requires government hosting providers to demonstrate certified levels of privacy, security and sovereignty; and
- reform of the **Privacy Act 1988** is tightening obligations, increasing penalties for serious breaches and giving individuals more control over their personal information.

Many organisations are now reviewing where their data lives, moving towards hybrid models anchored in Australian sovereign infrastructure.

Trust is earned where your data lives.

# What makes a data centre sovereign

The Australian Government's **Hosting Certification Framework** sets three levels: Strategic, Assured and Uncertified. Strategic is the highest, and only a small number of facilities and enclaves in Australia hold it. Requirements include:

| REQUIREMENT                  | WHAT IT MEANS                                                                                   |
|------------------------------|-------------------------------------------------------------------------------------------------|
| <b>Ownership and control</b> | Ownership and control held by trusted parties whose interests align with the Commonwealth       |
| <b>Personnel clearance</b>   | Key staff with unescorted access hold AGSVA clearance, to a minimum of Negative Vetting Level 1 |
| <b>Certification</b>         | Alignment with Australian standards and recognised certifications such as ISO/IEC 27001         |
| <b>Physical security</b>     | Facilities constructed to zone specifications in the Protective Security Policy Framework       |
| <b>Data protection</b>       | Data protected at rest, in transit and during processing                                        |
| <b>Ongoing compliance</b>    | A demonstrated, continuing commitment to privacy and protection obligations                     |
| <b>Monitoring</b>            | Secure systems monitoring security and availability across the whole facility                   |

**Why this matters to you:** when a provider says "sovereign", ask which certification level its facilities hold, who holds it, and what scope it covers.

Ask who holds the certificate, and for what.

# Five reasons to host sovereign

- 1 Cybersecurity**  
Local infrastructure aligned to recognised standards such as ISO/IEC 27001, without exposure to unfamiliar offshore threat environments.
- 2 Physical security**  
Cleared personnel and controlled access protect the premises where your data physically lives.
- 3 Compliance**  
Data maintained and processed onshore makes it simpler to meet Australian privacy and data obligations as they evolve.
- 4 Resilience**  
Redundant infrastructure designed to keep running through maintenance and resist outages, for services that cannot stop.
- 5 Reputation**  
Customers know where their information lives and who can access it. Transparency builds trust, and trust builds business.

Sovereign hosting is not only defensive. It is a visible commitment to the people whose information you hold.

Security you can explain to your customers.

# Does your organisation need it?

Most organisations benefit from sovereign infrastructure. The question is how high it should sit on your agenda.

## It may be less urgent if you

- ☐ Operate only in Australia
- ☐ Deal only with Australian customers and partners
- ☐ Collect and keep data only within Australia
- ☐ Use Australian-hosted cloud services
- ☐ Already follow all relevant privacy and security obligations

## It should be a priority if you

- ☐ Hold sensitive personal, health or financial records
- ☐ Must comply with sector regulation or government contracts
- ☐ Operate internationally or share data across borders
- ☐ Are adopting AI tools that process your documents
- ☐ Cannot say who could compel access to your data

## Sectors where it matters most

| SECTOR                          | WHY                                                        |
|---------------------------------|------------------------------------------------------------|
| Healthcare                      | Highly sensitive records and strict compliance obligations |
| Financial services              | Customer financial data and regulatory scrutiny            |
| Government and suppliers        | Hosting requirements flow down through contracts           |
| Legal and professional services | Client confidentiality and privilege                       |
| Community and not-for-profit    | Vulnerable clients and donor trust                         |

# Sovereign AI explained

Generative AI is now part of everyday work. With that opportunity come new risks: ethics and bias, job disruption, and growing dependence on technology built elsewhere for someone else's context.

**Sovereign AI** is AI built and operated using a nation's own infrastructure, data and workforce, under its own laws, to serve its own interests. It sits within the wider idea of digital sovereignty, which holds that technology which shapes society should remain answerable to that society.

## SECURITY

### Control of the stack

Prevents foreign intervention and manipulation of critical AI systems.

## PRIVACY

### Data stays home

Citizens' and customers' information remains within national borders.

## ECONOMY

### Local capability

Builds domestic innovation, skills and industry.

## ADVANTAGE

### Local problems, local answers

AI tuned to national context, language and priorities.

For a business, sovereign AI starts with a simple principle: your data should not leave your control to make your AI work.

Your AI. Your data. Your jurisdiction.

# What sovereign AI requires

| REQUIREMENT               | WHAT IT INVOLVES                                                                                                            |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>Infrastructure</b>     | Data centres built to supply the power, cooling and protection that accelerated computing needs, keeping processing onshore |
| <b>Compute and models</b> | Capacity to run and adapt models within national borders                                                                    |
| <b>Data</b>               | Robust, well-governed datasets that reflect local context                                                                   |
| <b>Workforce</b>          | Skilled engineers and data scientists, and an education pipeline to grow them                                               |
| <b>Ethics</b>             | Clear frameworks for privacy, accountability, transparency and protection                                                   |
| <b>Dialogue</b>           | Open conversation between business, government and international partners on shared standards                               |

## The challenges

### COST

#### Infrastructure is expensive

Sovereign capability takes sustained investment in facilities, data and people.

### TALENT

#### Skills are scarce

Smaller nations must grow local expertise while staying open to collaboration.

### ETHICS

#### Guardrails matter

Domestic control must come with strong oversight to prevent misuse.

### BALANCE

#### Self-reliance and cooperation

Sovereignty should not mean isolation from global progress.

# Sovereign AI around the world

Governments are already investing. As reported in 2024:

## INDIA

### National compute

Approved around US\$1.24 billion for a sovereign AI platform, including a supercomputer of at least 10,000 GPUs.

## JAPAN

### AI infrastructure

Pledged around US\$740 million to subsidise domestic AI supercomputers and Japanese language models.

## SINGAPORE

### Local language models

Developing a sovereign large language model reflecting local and regional cultures under its National AI Strategy.

## TAIWAN

### Trusted dialogue

Building TAIDE, a government-funded model adapted to local sources to counter politically biased tools.

## What it means for Australia

The lesson for Australian organisations is not that every business needs its own model. It is that the infrastructure, data and governance behind AI are strategic assets. Choosing Australian-hosted, Australian-managed platforms is a practical way to take part in AI without giving up control.

Sovereignty is now a competitive advantage.

# How we build: a view from our CTO

Shaune Irving, Chief Technical Officer

Sovereignty is easy to claim and hard to engineer. At Keytech we treat it as an architecture decision made on day one, not a setting switched on before launch.

| LAYER         | HOW KEYTECH APPROACHES IT                                                                                                    |
|---------------|------------------------------------------------------------------------------------------------------------------------------|
| Hosting       | Australian Managed Azure through Macquarie Cloud Services, with Macquarie private cloud available for workloads that need it |
| Connectivity  | Private, dedicated links into the hosting environment where a client needs traffic kept off the public internet              |
| Identity      | Microsoft Entra ID single sign-on, multi-factor authentication and role-based access                                         |
| Isolation     | Each client in its own environment, with no commingling of data                                                              |
| AI processing | Requests routed to approved models inside the controlled environment; client data is not used to train public models         |
| Audit         | A record of who asked, what was retrieved, which model answered and what was returned                                        |
| Controls      | The ASD Essential Eight applied today, with our roadmap aligned to ASD's new Essentials series                               |

Our team is small, fast and precise. We design for organisations that operate in high-risk environments, where a wrong answer or an exposed record has real consequences, and we hold every platform we build to that standard.

Keytech is also a partner in the Australian Signals Directorate's Cyber Security Partnership Program, which keeps us close to current ASD threat advice and guidance as it changes.

**Infrastructure note:** ISO/IEC 27001 and IRAP assessment at PROTECTED are held by Macquarie for its infrastructure services.

# From Essential Eight to Essentials

For almost a decade the **ASD Essential Eight** has been the baseline Australian organisations used to measure their cyber security. That is now changing. In June 2026 the Australian Signals Directorate announced that the Essential Eight will be retired and replaced by a broader **Essentials series**.

The reason is simple. The Essential Eight was designed for on-premises IT, before cloud, software-as-a-service and AI became part of everyday work. The Essentials series moves from a fixed list of technical controls to outcome-based guidance across distinct domains.

## CHAPTER ONE

### Enterprise IT

The direct successor to the Essential Eight, and the first chapter of the series.

## TO FOLLOW

### Cloud

Guidance built for shared-responsibility and SaaS environments.

## TO FOLLOW

### Operational technology

Security for the systems that run physical operations and infrastructure.

## ON THE HORIZON

### Artificial intelligence

Expected guidance for AI and agentic systems as they enter the workplace.

## What the transition looks like

| STAGE            | REPORTED TIMING                                                                         |
|------------------|-----------------------------------------------------------------------------------------|
| Now              | Essential Eight remains live and current, running alongside the new Essentials guidance |
| Around 12 months | Essential Eight begins to be deprecated                                                 |
| Around 24 months | Essential Eight is retired as a whole                                                   |

**What it means for you:** keep going with any Essential Eight work already under way. Most existing controls map into the new framework. Plan your next uplift around Essentials, particularly for cloud and AI.

# Launch AI by Macquarie

Sovereign AI used to mean building your own infrastructure. **Launch AI**, from Macquarie Cloud Services, changes that. It runs generative AI as a governed service, delivered entirely from Australian sovereign private cloud.

## SOVEREIGN

### Data stays onshore

Data, prompts and operational logs remain within Australia's borders.

## PREDICTABLE

### Fixed monthly capacity

Priced on capacity rather than volatile token usage, so AI costs can be forecast.

## OPEN

### No model lock-in

A central model-as-a-service layer connects applications through open integration, avoiding siloed AI.

## GOVERNED

### Enterprise-ready

Identity-aware access, governance guardrails and observability built in from day one.

## From pilot to production

Many organisations get stuck between an AI experiment and a working service. Launch AI is designed to bridge that gap: start in a shared environment to prove a use case, then move to dedicated capacity as AI becomes business-critical, without rebuilding the architecture.

Because it runs alongside private cloud workloads, AI sits close to the data it uses. That reduces data movement, latency and public cloud egress charges.

For Keytech clients, Launch AI is a sovereign option for running AI inside Australia, under Australian control, at a cost the business can plan for.

Sovereign AI, as a service.

# Private cloud and private connectivity

Not every workload belongs on shared public cloud. Through our partnership with Macquarie, Keytech can host client environments on **Macquarie's Launch private cloud**, in Australian-owned and operated Tier III data centres, as well as on Australian Managed Azure.

| OPTION                          | BEST SUITED TO                                                                                                       |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------|
| <b>Australian Managed Azure</b> | Organisations that want the Microsoft ecosystem with data kept onshore and managed by an Australian provider         |
| <b>Macquarie private cloud</b>  | Sensitive or critical workloads that need dedicated capacity, predictable performance and fixed monthly cost         |
| <b>Hybrid</b>                   | Organisations that want to keep some systems where they are while moving critical data onto sovereign infrastructure |

## Private express connectivity

For organisations that do not want sensitive traffic crossing the public internet, we can connect your sites and systems to your hosted environment over **private, dedicated network links**. Data travels on a private path from your office or data centre straight into your Keytech environment.

### SECURITY

#### Off the public internet

A smaller attack surface for your most sensitive traffic.

### PERFORMANCE

#### Consistent speed

Predictable latency and throughput for everyday work and AI.

### CONTROL

#### Known path

You know exactly how your data reaches its destination.

### COMPLIANCE

#### Easier to evidence

A clear story for auditors, boards and government contracts.

# Assess your data position

Take these questions to your next leadership or board meeting. If you cannot answer one with confidence, that is where to start.

## Where and whose

- ☐ Where is our data stored, and where is it processed?
- ☐ Which country's laws apply to each provider we use?
- ☐ Could a foreign authority compel access to our data?
- ☐ Who owns and operates the infrastructure?

## Resilience

- ☐ How quickly could we recover from a breach or outage?
- ☐ Are backups held onshore and tested?

## Who and how

- ☐ Who has access, and how is it controlled and logged?
- ☐ What policies govern data shared with partners?
- ☐ Do our AI tools send documents offshore or use them for training?
- ☐ Who holds each certification our providers claim, and for what scope?

## Readiness

- ☐ Are we prepared for Privacy Act reform?
- ☐ Is our cyber plan ready for ASD's move to Essentials?

Know where your data lives.

# How Keytech can help

Every organisation starts from a different place. Whether you are reviewing a single system or planning how to adopt AI safely, we can help you understand your position and act on it.

## REVIEW

### Data position review

A practical assessment of where your data lives, which laws apply and where the gaps are.

## PLAN

### Sovereign roadmap

A clear, staged plan to bring critical workloads onto Australian-managed infrastructure.

## SECURE

### Essential Eight to Essentials

Uplift against the Essential Eight today, with a clear path to ASD's new Essentials series.

## HOST

### Private cloud and connectivity

Sovereign hosting on Macquarie infrastructure, with private links that keep traffic off the internet.

## ADOPT

### Sovereign AI

Secure AI on Australian infrastructure, including Launch AI by Macquarie, keeping your data in your control.

## ONBOARD

### Keytech Core

A guided move onto Keytech Core, our secure platform for organised knowledge and AI. See over the page.

If you are not sure where your data sits today, that is the best reason to talk to us. A conversation costs nothing and could change how you see your risk.

## TALK TO US

**Luke Lispet**, Chief Executive Officer · [luke@keytechintelligence.ai](mailto:luke@keytechintelligence.ai)

**Shaune Irving**, Chief Technical Officer

(07) 3063 7575 · 22 Magnolia Drive, Brookwater QLD 4300 · [keytechintelligence.ai](https://keytechintelligence.ai)

# Onboarding into Keytech Core

**Keytech Core** is our secure platform that brings an organisation's documents, knowledge and AI together in one controlled environment, hosted in Australia. Every answer is linked back to its source, and every action is recorded.

Onboarding is guided by our team from first conversation to go-live. You do not need in-house AI expertise to get started.

- 1 Discovery**  
We learn how your organisation works, what information you hold and what you want to improve.
- 2 Environment setup**  
We provision your own isolated environment on Australian infrastructure, with private connectivity if you need it.
- 3 Identity and access**  
We connect Microsoft Entra ID for single sign-on and set roles so people see only what they should.
- 4 Knowledge and data**  
We bring in your documents and knowledge sources securely, organised the way your teams already work.
- 5 Configuration**  
We set up your workflows, approved AI models and audit settings to match your policies.
- 6 Training and go-live**  
We train your people, run a supported pilot, then move to full use with ongoing support.

Identity, documents, knowledge, AI, source, action, audit. Every step stays inside your environment.



# Sovereign by Design.

Secure, sovereign technology and AI for Australian organisations.

## PARTNERS AND PROGRAMS



Microsoft



macquarie  
CLOUD SERVICES



macquarie  
TECHNOLOGY GROUP



NVIDIA  
INCEPTION PROGRAM

ASD

AUSTRALIAN  
SIGNALS  
DIRECTORATE

*Veteran Owned, Australian Owned, Small Business scaling with purpose for organisations that operate in high risk environments.*

(07) 3063 7575 · [contact@keytechintelligence.ai](mailto:contact@keytechintelligence.ai) · [keytechintelligence.ai](https://keytechintelligence.ai)  
22 Magnolia Drive, Brookwater QLD 4300

Acknowledgement: this publication has been informed and influenced by the Macquarie Data Centres knowledge hub, in particular its articles "A Guide to Australian Data Centre Sovereignty" and "Sovereign AI" (September 2024). Essentials transition timing as reported by ASD in June 2026. Launch and Launch AI are products of Macquarie Cloud Services. Partner marks indicate partnership and program participation, not endorsement. This guide is general information, not legal or compliance advice. © 2026 Keytech Intelligence Pty Ltd, ABN 30 700 316 169.