



# Policy for the **responsible use of artificial intelligence** in the Tasmanian Government

## Part 3 – Requirements for agencies

July 2026 | Version 1.0

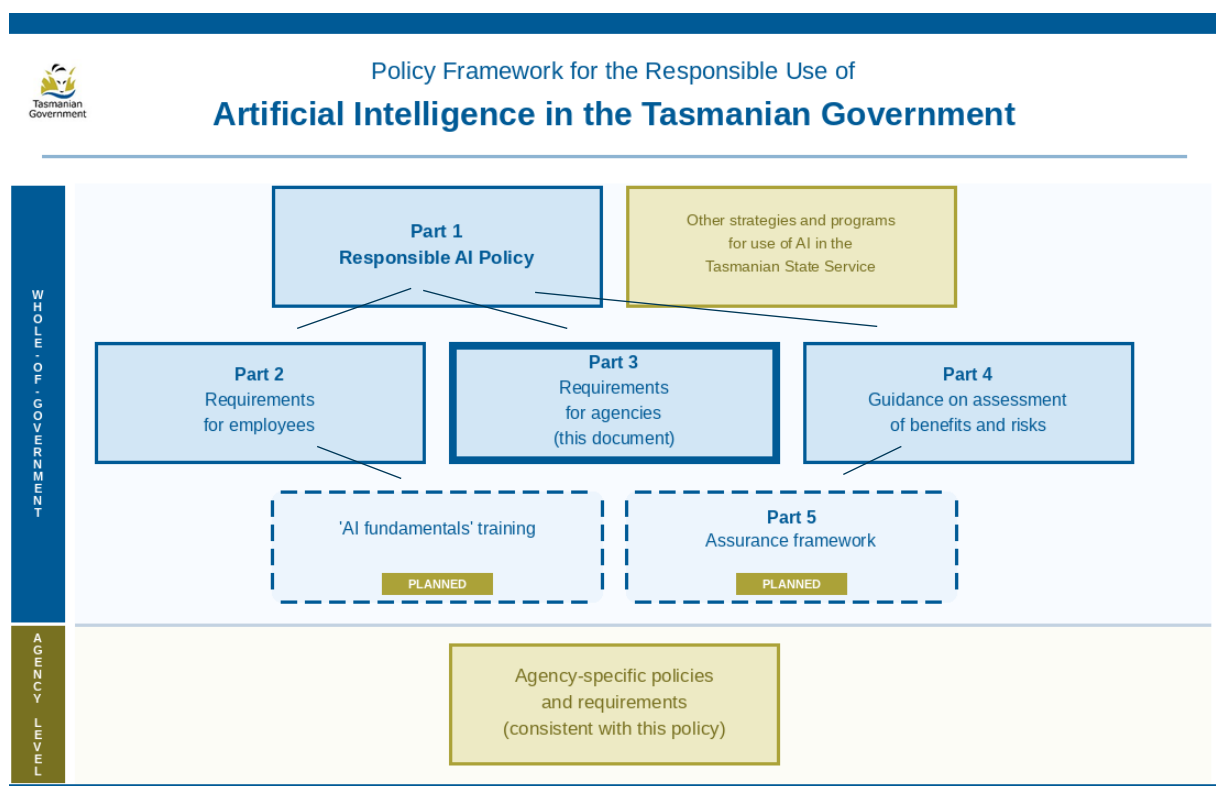
# Purpose

This policy establishes a consistent ‘baseline’ approach to the use of AI by the Tasmanian Government, so that agencies can harness its benefits, while ensuring its use is **ethical**, **responsible**, and **safe**. This is essential for public trust in government use of AI.

Each government agency remains responsible for its own oversight, assurance, and implementation.

# Elements

The policy framework is set out here:



Part 3 of this policy provides guidance for agencies to support effective implementation. It is designed mainly for Tasmanian Government executives and managers. It sets out:

- Mandatory requirements, and
- Recommended actions.

Agencies should also review Part 4 of this Policy - Guidance on assessment of benefits and risks.

# Compliance statements

The agency:

- ✓ can demonstrate that it does not use AI tools to make final decisions.
- ✓ has assigned responsibility for implementing this policy to one or more accountable officials (AOs) within six months of the policy taking effect
- ✓ has published a short transparency statement explaining its approach to adopting and using AI within six months of this policy taking effect
- ✓ has reviewed its AI transparency statement annually and updated as needed
- ✓ has provided brief summaries of any AI projects, systems, or uses classed as Mid-Range Risk or higher to the Data and Digital Committee (DDC), for inclusion in an AI Register, within six months of this policy taking effect
- ✓ has reviewed its reporting to the AI Register annually and updated as needed
- ✓ has set risk tolerances for its use of AI that align with its risk-management policy
- ✓ ensures that employees who develop, deploy or operate AI systems have the appropriate training, skills and support
- ✓ provides clear guidance to employees on which AI systems and tools are authorised for official use
- ✓ has consulted the Office of the Crown Solicitor on any mandatory requirements for procurement and contracting of AI, including where AI is used by suppliers, consultants or contractors.

## Requirements for all Tasmanian Government agencies

### Requirements – summary

1. Set strategic priorities for use of AI.
2. Establish accountabilities and assurance processes to identify and manage risks.
3. Grow capability.
4. Align procurement and contracts with responsible deployment and assessment of risk.
5. Cooperate and collaborate with other Tasmanian Government agencies and relevant external partners.

# Requirements – detail

## 1. Set strategic priorities for use of AI

### Why is this important?

Tasmanian Government agencies need to engage with AI confidently, safely and responsibly, and realise its benefits.

The value proposition for AI-powered automation and advanced decision support is well accepted across industry and (increasingly) in government.

For Tasmanian Government agencies, AI is likely to deliver significant efficiency and productivity benefits by:

- simplifying and automating processes
- improving service design and delivery, and
- enhancing policy development by analysing and organising large volumes of unstructured information.

It is important that agencies take a balanced view of the opportunities and risks. As with other technologies, AI can involve both low- and high-risk situations. Many AI deployments will offer strong opportunities for productivity and innovation and will not be high risk.

For many organisations, AI is most likely to be adopted through the introduction and integration of AI features within suppliers' products and service offerings.

These requirements do **not set the strategic framework or priorities for AI use across the Tasmanian State Service. These will be developed through other processes.**

### Mandatory requirements

Nil.

## Recommended actions

Conduct regular environmental scans and gap analyses to identify current and emerging AI capabilities and the potential benefits they may offer for agency operations. This may include ongoing engagement with other Tasmanian Government agencies and with counterpart agencies in other jurisdictions.

Develop strategies and implementation plans for any prioritised AI capabilities, in line with this policy.

## 2. Establish accountabilities and assurance processes to identify and manage risks

### Why is this important?

To have clear accountabilities for the adoption of AI, and to understand its use.

To ensure AI use in the Tasmanian Government is ethical, responsible, transparent, and explainable to the public.

To ensure AI risk mitigation is proportionate and targeted.

To ensure agencies can explain, justify, and take ownership of advice and decisions that involve AI.

To recognise that when AI systems use machine learning, they may continue to change *after* deployment and require active monitoring throughout their lifecycle.

See also [Part 4 of this Policy - Guidance on assessment of benefits and risks](#).

## Mandatory requirements

### Decision making

Ensure your agency does not use AI tools to make final decisions. These tools may only support decision-making. Final decisions must always be made by an authorised and fully informed person, or delegate. **This requirement is critical.** If it is not met, there is a high risk of error; actual or reputational harm; and administrative or judicial review.

### Accountable Officials

Agencies must assign responsibility for implementing this policy to one or more accountable officials (AOs) within **six months** of the policy taking effect.

## Choosing one or more AOs

These responsibilities may be assigned to an individual, or to the chair of a committee or governance body.

Agencies may choose to distribute AO responsibilities across several senior leaders or existing roles - such as a Chief Information Officer, Chief Technology Officer, or Chief Data Officer.

Because implementing this policy is not only a technical task, AOs may also come from business or policy areas.

AOs should have enough authority and influence to drive the policy's implementation effectively within their agency.

## AO responsibilities<sup>1</sup>

As a key leadership role, AOs are to:

- take responsibility for implementing this policy within their agency
- act as the main point of contact within the agency, and the main external contact for whole-of-government AI coordination
- oversee the management of identified AI risks within the agency's existing risk-management frameworks (see Part 4 of this Policy - Guidance on assessment of benefits and risks)
- promote a culture that balances AI risk management with innovation
- participate in whole-of-government AI forums and processes
- support the development of, or alignment with, an agency-specific AI policy
- stay informed about changing requirements as they evolve
- periodically review how the policy is being implemented and provide feedback or suggestions to the Tasmanian Government Data and Digital Committee (DDC), as required

The policy does not make AOs responsible for the agency's AI use cases.

## AI Transparency Statement

Agencies must publish a short statement on their public facing website explaining their approach to adopting and using AI within **six months** of this policy taking effect.

The statement should give the public some brief, clear information about the agency's use of AI, including:

---

<sup>1</sup> Adapted from Australian Government, Digital Transformation Agency (2024), [‘Standard for accountable officials: Supporting the policy for responsible use of AI in government’](#)

- how the agency complies with this policy
- how it monitors the effectiveness of AI systems in use
- the steps it takes to protect the public from negative impacts.

It is recommended that this statement focus on any AI uses assessed as Mid-Range Risk or higher. For AI risk classifications, see [Part 4 of this Policy - Guidance on assessment of benefits and risks](#).

Agencies should note that AI Transparency Statements are now required for all Australian Government agencies and are available on their websites. An example is published by the [Australian Government Department of Home Affairs](#).

A template will be provided as an optional resource that agencies may adapt and customise.

The statement must be **reviewed annually** and updated as needed. It should also be updated sooner if the agency makes significant changes to its approach or use of AI.

## Register of AI Applications (mid-range risk or higher)

Agencies must provide brief summaries of any AI projects, systems, or uses classed as Mid-Range Risk or higher to the DDC, for inclusion in an AI Register, within **six months** of this policy taking effect.

This enables the Tasmanian Government to:

- identify best practice in AI risk management
- identify and address common areas of concern
- be confident that any potential risks to government or the community have been identified and are being mitigated.

For AI risk classifications, see Part 4 of this Policy - Guidance on assessment of benefits and risks.

An abridged version of the AI Register may be made public.

In cases where it is not appropriate to provide detail on specific AI applications (for example for security or law enforcement purposes), these may be referred to in general terms. These uses remain subject to existing agency accountability and reporting mechanisms.

At a minimum, these summaries should include:

- a brief description of the project and how AI is used
- key ethical considerations taken in designing the project
- a contact point for the project.

A reporting template will be provided as an optional resource that agencies may adapt and customise.

The Secretariat of the DDC will manage details of this reporting arrangement. This includes requesting and collecting information, and administration of the public facing register.

The Register must be **reviewed annually** and updated as needed. It should also be updated sooner if an agency makes significant changes.

## **Risk tolerances and risk assessments**

Set risk tolerances for the use of AI that align with your agency's risk-management policy.

See [Part 4 of this Policy - Guidance on assessment of benefits and risks](#).

## **Monitor and evaluate**

Regularly review the agency's internal policies and governance arrangements for AI to ensure they remain appropriate and effective.

Monitor AI use cases to identify any unintended impacts.

Note that where AI systems use machine learning, they may continue to change *after* deployment and require active monitoring throughout their lifecycle.

## **Recommended actions**

### **Compliance, escalation and accountability**

Agencies are responsible for managing their own processes for:

- ensuring employees understand and follow legislative and administrative requirements for using AI
- escalating and resolving issues
- clarifying the accountabilities of individual employees, line managers, and executives.

## **AI assurance and risk assessment**

Until the Tasmanian Government's AI Assurance Framework is released, agencies are strongly encouraged to use:

- Part 4 of this Policy - Guidance on assessment of benefits and risks.

- [National framework for the assurance of artificial intelligence in government](#)
- [NSW Artificial Intelligence Assessment Framework](#)

If agencies are unsure how to approach AI assurance or risk assessment, they should seek advice from the Tasmanian Government Chief Information Officer or through the DDC.

## **Alternative assurance paths**

In specialist areas, AI used in commercial products for specific purposes may already be regulated under existing laws. For example, certain AI applications used in medical or clinical settings may require approval from the Therapeutic Goods Administration (TGA).

In such cases, agencies are encouraged to review relevant national frameworks and manage their own internal policies and assurance processes.

To maintain complete oversight and reporting, agencies must still:

- prepare an AI Transparency Statement, and
- list any AI systems that follow an alternative assurance path on the Tasmanian Government Register of AI Applications if they have been assessed as mid-range risk or higher.

## **Consider AI impacts for other frameworks**

Include AI-related considerations in existing agency frameworks, such as those for privacy, protective security, record keeping, cyber security, and data management.

## **Whitelisting**

Agencies may choose to exempt, or whitelist, certain solutions from detailed risk assessment when it is clear they meet responsible AI requirements and preliminary analysis shows the risks are low.

Agencies may choose to recognise whitelisting decisions made by other Tasmanian agencies, or by agencies in other jurisdictions.

### 3. Grow capability

Tasmanian Government capability for the responsible use of AI includes both technical and human capability.

**Technical** capability will be developed mainly through agency strategies and coordinated, where needed, by the Data and Digital Committee.

This policy focuses on building **human** capability across the Tasmanian State Service.

#### Why is this important?

To support a successful transition to AI-enabled ways of working, employees need regular communication and consultation; and access to AI tools, training and support - relevant to their roles.

This is essential for improving productivity and providing opportunities for employees, while avoiding a 'digital divide' in the Tasmanian Government workforce.

Employees must be able to explain, justify and take ownership of advice and decisions that involve AI.

Employees should understand what AI can and cannot do - and be aware of the potential risks.

AI systems currently lack reasoning and contextual awareness, and their limitations vary depending on the tool and the context. AI systems are not guaranteed to be accurate.

Employees need to know how to use AI tools safely and responsibly; apply methods to increase accuracy and correctness; and to test outputs, when required.

#### Mandatory requirements

Agencies must ensure that employees who develop, deploy or operate AI systems have the appropriate training, skills and support.

This includes understanding:

- principles and requirements for responsible AI deployment
- AI capabilities, limitations and risks
- the types of critical thinking needed when using AI.

Agencies must provide clear guidance to employees on which AI systems and tools are authorised for official use.

## Recommended actions

- Provide most employees, regardless of role, AI fundamentals training aligned with this policy, once available.
- Consider whether employees need additional, subject-specific AI training relevant to their field of work.
- Engage with whole-of-government capability-building initiatives to support skills development.
- Consider working with equivalent agencies in other Australian jurisdictions to develop and share subject-specific training materials.
- Provide AI refresher training to reinforce learning and cover new developments.
- Provide further training for employees whose roles involve procurement, development, training or deployment of AI systems.

## 4. Align procurement and contracts with responsible deployment and assessment of risk

### Why is this important?

Many Tasmanian Government projects and services rely on external consultants and contractors. Increasingly, these providers - and their subcontractors - use AI as part of their service delivery. Many ICT products and services now include AI components.

It is important to have visibility and control over how suppliers use or integrate AI into the deliverables, solutions or services they provide. Agencies need clear visibility and control over how suppliers and service providers use or integrate AI into the solutions, services or deliverables they provide. This includes safeguarding data sovereignty and intellectual property.

Without adequate safeguards, this can create areas of risk for government, particularly if external consultants and contractors do not use AI responsibly.

There are three main procurement use cases:

- procuring services where the supplier may use AI systems to deliver the service
- developing an AI tool within the agency, with support from a consultant (including tools for automated decision making)
- procuring a software product with embedded or integrated AI capabilities.

### Mandatory requirements

Consult the Office of the Crown Solicitor on any mandatory requirements for procurement and contracting.

The Digital Transformation Agency (DTA) has issued [model contract clauses](#) to support Australian Government agencies when procuring AI systems, AI-enabled products, or service providers who support internal AI development.

Agencies must consult the Office of the Crown Solicitor to confirm whether these clauses, or any other requirements, should be applied to suppliers, consultants or contractors using AI.

## 5. Cooperate and collaborate

### Why is this important?

Some AI systems - such as generative AI platforms used for common administrative tasks - may be more effective when requirements, procurement, and implementation are coordinated across government.

Loss of public trust in government use of AI is unlikely to be limited to one agency. This risk can be reduced through strong oversight from the DDC and ongoing collaboration on best practice.

Government agencies across Australia are facing similar challenges. To reduce duplication of effort, Tasmanian Government agencies can benefit from identifying opportunities to collaborate with equivalent agencies in other jurisdictions.

To keep Tasmanian Government customers - including businesses and the community - at the centre of service delivery, agencies should engage early, regularly and meaningfully with stakeholders when introducing AI-assisted technologies that affect service delivery.

### Mandatory requirements

Contribute to the whole-of-government Register of AI Applications (mid-range risk or higher).

### Recommended actions

Commit to a culture of collaboration and knowledge sharing across agencies and across government on matters related to AI. This includes:

- participating in co-design of policy, standards and guidance
- supporting alignment of approaches for assuring government use of AI
- creating ways to share knowledge, such as AI solution patterns, joint projects, or examples of new risks, effective mitigation measures and lessons learned
- responding to new opportunities and risks, technical developments, legislative changes, and national or international developments
- adopting and contributing to the Tasmanian Government AI Glossary
- Collaborate with equivalent agencies in other Australian jurisdictions to develop and share subject-specific policy, assurance processes, and training materials.

Consider frameworks that help define the roles and responsibilities of internal and external stakeholders involved in, or affected by, government use of AI. These may include tools such as the RACI model, which identifies whether stakeholders are Responsible, Accountable, Consulted or Informed.

Look for opportunities to draw on expertise from across disciplines relevant to the responsible use of AI. This may include public sector leaders, managers, employees, and specialists in strategy, policy, ethics, technology and law.

## Useful resources

- Australian Government, Digital Transformation Agency – [Artificial Intelligence \(AI\) Model Clauses, 2019, Version 2.0](#)
- Australian Government, Department of Finance - [National framework for the assurance of artificial intelligence in government, June 2024](#)
- Australian Government, Digital Transformation Agency - [Standard for AI transparency statements, 2024, Version 1.1](#)
- New South Wales Government, Digital NSW - [NSW Artificial Intelligence Assessment Framework, July 2024](#)
- Australian Government, Department of Industry, Science and Resources – [National AI Plan, 2025](#)

## AI Use and Readability Disclosure

This policy includes text revised with Microsoft 365 Copilot to about Year 9 readability. The target reflects Australian Government Style Manual guidance to write for lower-secondary readers and supports ISO 24495-1:2023 (Plain language) principles. All revisions underwent human review for accuracy.