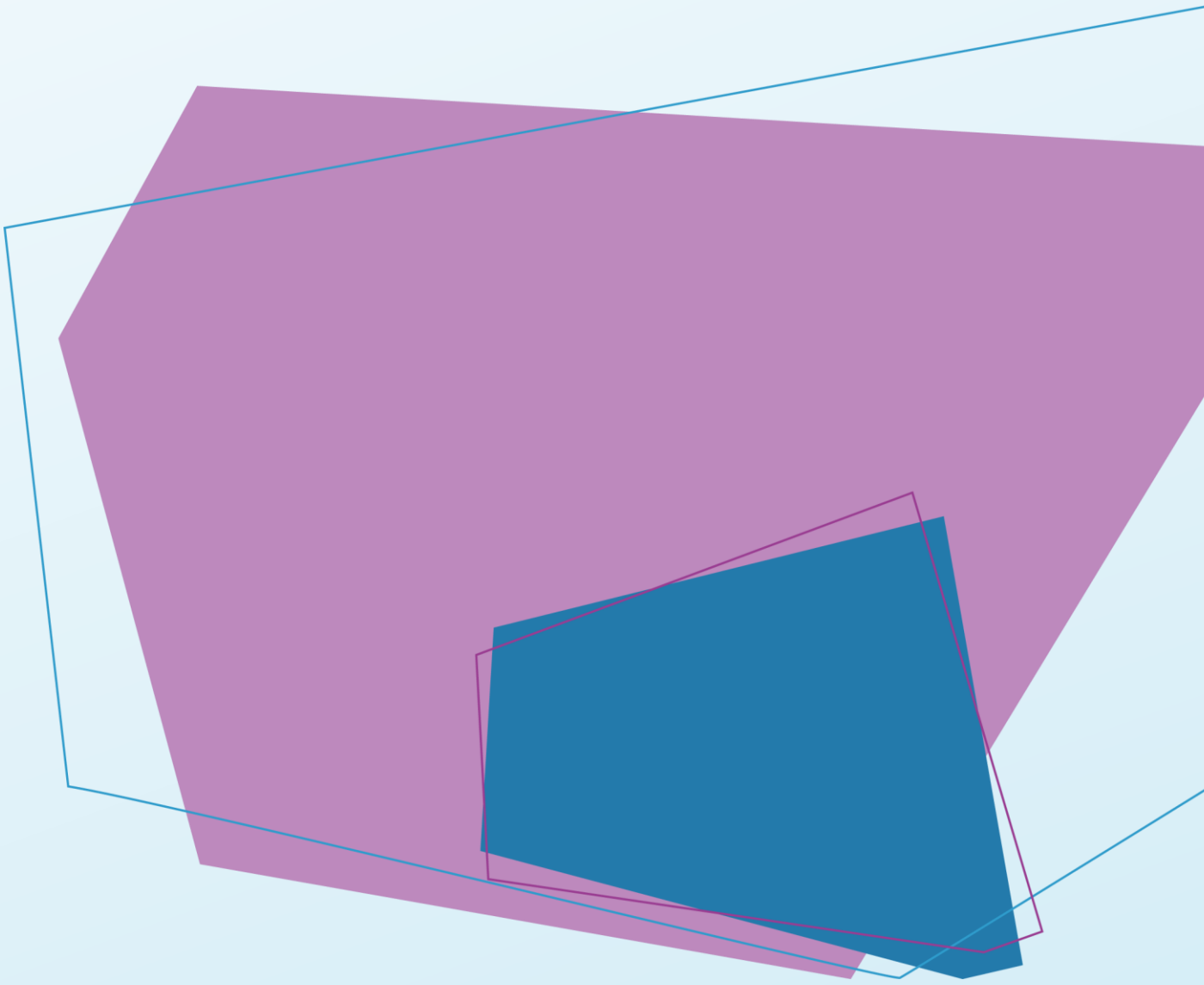
Australian Government
Department of Industry, Science and Resources

National Artificial Intelligence Centre

# AI policy guide and template

v1.0, October 2025



industry.gov.au/NAIC

# Introduction

> Organisations who use AI should develop and maintain an AI policy. An AI policy is your organisation's essential guiding resource for all AI-related activities.

Developing and implementing an AI policy is fundamental to effective AI governance. An AI policy sets out your organisation's commitment to using AI responsibly. And it acts as a reference for staff, stakeholders and auditors who want to understand your organisation's approach to AI.

This template is a starting point for writing your organisation's AI policy. The example text we've included in this template is a good baseline for any AI policy. It aligns with the government's *Guidance for AI Adoption*, and will set up your organisation to use AI responsibly and consistently.

The template includes core principles, expectations and rules for the development, deployment and use of AI systems. You should adapt the template so your AI policy reflects your organisation's values, industry standards and legal obligations.

## Using the template

The template sets out a recommended structure and includes example content to help you get started.

You should:

- **align the statements** with your organisation's core values and mission
- **define roles and responsibilities** that match your existing organisational and governance structures
- **modify terminology** to align with your organisation's internal language
- **seek feedback** to ensure the AI policy is fit for purpose.

# Purpose

> Every AI policy should start with a high-level purpose which explains your organisation's strategic goals for AI use.

**Editing suggestion:** customise the bullet points to align with your organisation's AI strategic goals. Remember to include versioning details, including the last date of update.

## Example text

AI policy version date: *[Date of last update to the policy]*

The *[organisation name]* AI policy establishes principles for the ethical, responsible and effective use of AI systems. It ensures alignment with our mission and values.

Specifically, this policy aims to:

- protect the rights of stakeholders
- support the use of AI to enhance service delivery and achieve our strategic objectives
- ensure transparency in our AI practices so we can maintain public confidence
- provide a clear risk framework for identifying, assessing and managing the risks associated with AI systems
- engage and empower our staff.

# Scope

> Clearly defining the scope of your AI policy is important. It should align with your organisation's structure and reflect the intended breadth of coverage – whether across departments, functions or organisation-wide.

**Editing suggestion:** Customise the first section to match your organisation's structure and your desired scope of coverage.

If you edit the definition of an 'AI system', make sure your changes capture any technology that introduces AI-specific risks (like inheriting bias from data, lack of explainability or autonomous behaviour) that this policy is designed to manage. We have deliberately used a simplified definition to make it easier to understand. You can also use other definitions if they are more appropriate to your organisation.

## Example text

This policy applies to:

- all **employees, volunteers, contractors and board members** involved in the development, adoption, management, or use of AI systems at our organisation
- all AI technologies under *[the organisation's]* control, including those developed in-house, purchased from vendors or embedded within larger software platforms including cloud-based systems.

We define an **AI system** as any technology that uses data to make inferences and generate outputs such as predictions, recommendations, or decisions with a degree of autonomy.

This includes, but is not limited to:

- machine learning models
- generative AI tools
- predictive analytic systems
- chatbots that generate their own responses.

It excludes:

- standard spreadsheet formulas
- rule-based automations (such as 'if–then' macros)
- traditional business intelligence dashboards.

If you are uncertain about whether an AI technology falls under this policy, consult the AI policy owner.

# Policy statements

> Policy statements form the core of your policy. They set out the principles and expectations that guide how AI is designed, adopted and used throughout your organisation.

**Editing suggestion:** We have based the example text on common AI ethics frameworks. You should make sure they reflect your organisation's specific values, industry standards, other policies and legal obligations. Make sure these statements can be translated into actions.

## Example text

The following AI governance statements set out *[organisation name's]* expectations for the responsible design, adoption and use of AI systems across the organisation. They should guide decision-making, promote ethical practices, and ensure AI use aligns with our mission, values, and stakeholder obligations.

These statements apply to all AI systems within scope and must be interpreted in conjunction with our broader risk management, privacy, and technology governance frameworks.

### 1. Ethical and human-centered use

AI systems must align with our values, respect human dignity and empower human judgment for ultimate decision making.

All uses of AI systems must reflect Australia's AI Ethics Principles and our values and contribute positively to our mission. AI must not be used to deceive or manipulate stakeholders.

### 2. Clear accountability

Each AI system must have an accountable person with sufficient understanding of the system who is responsible for its outcomes and compliance with this policy.

An accountable person must be chosen before any AI system is adopted. For systems that involve third parties (such as vendors or developers) responsibilities must be clearly documented across the supply chain.

## 3. Risk and impact assessment

An AI system must go through a risk and impact assessment before we begin to use it. There must be controls in place that are appropriate the level of risk we are taking on.

Relevant stakeholders should be engaged to understand potential impacts, particularly on vulnerable or marginalised groups.

## 4. Quality, reliability and security

An AI system must go through rigorous testing before it is deployed to make sure it is secure and dependable. Once it is in use, it must be monitored continuously for performance issues and emerging risks.

Testing acceptance criteria should match identified risks and be clearly documented. All relevant privacy and security safeguards must also apply to AI systems handling sensitive data.

## 5. Fairness and inclusion

AI systems must be inclusive and accessible. They must not involve or result in unfair discrimination against individuals, communities or groups.

AI use should reinforce our commitments to diversity, inclusion and accessibility – not undermine them. We must be especially careful in use cases where decisions affect individuals from marginalised or vulnerable populations.

## 6. Transparency and contestability

AI use must be transparent. We must inform impacted parties where appropriate. We must also support them to understand and contest outcomes where relevant.

All approved AI systems must be clearly recorded in our AI register. We must keep relevant information about AI-assisted decisions that significantly affect people and, where appropriate, we must make it available upon request.

## 7. Human oversight and control

We must maintain human oversight over AI systems. Our oversight will increase in line with the potential impacts of the AI decisions on people or our organisation.

Users of AI systems are responsible for overseeing the quality of its outputs. Humans must be able to pause, override or shut down AI systems when necessary. Where critical services rely on AI systems, manual alternatives must be maintained in case the system fails or needs to be taken offline.

# Governance and compliance

> The governance and compliance section outlines key policy elements, starting with the clarification of roles and responsibilities across the organisation. This section should also include your procedures for new AI use cases as well as your approach to incident management.

## Roles and responsibilities

**Editing suggestion:** Customise these roles and responsibilities to fit your organisation's size and existing governance structure. For smaller organisations, one person may hold multiple roles.

### Example text

To ensure effective governance of AI systems, the following roles and responsibilities are established:

| Role | Definition | Responsibilities |
|---|---|---|
| **AI policy owner** | A designated senior leader who is the overall owner for AI, with the authority to govern its use across the organisation. | • Champions, sponsors and maintains the organisation's AI policy and its commitment to responsible AI use.<br>• Holds ultimate accountability for AI governance, including capabilities and risks.<br>• Ensures adequate training is available for those in AI accountability roles |

| Role | Definition | Responsibilities |
|---|---|---|
| **Policy approvers** | The individual or committee with the authority to formally approve this policy and its subsequent revisions.<br>This may be a specific person like the CEO or a group like the Board of Directors. Clearly state who holds this authority. | • Reviews and formally approves the AI policy, ensuring it aligns with the organisation's strategic goals, risk appetite, and legal obligations.<br>• Champions the policy from the highest level of the organisation to foster a culture of responsible AI use.<br>• Approves any significant amendments or updates to the policy over time. |
| **Compliance monitor** | The individual or team responsible for overseeing and verifying adherence to this AI policy.<br>This function could be assigned to a specific person, an existing team like Internal Audit or Risk and Compliance, or Head of Operations. | • Audits AI system documentation to verify that required steps, such as the Pre-Screening Triage and risk assessments have been completed.<br>• Monitors AI-related incident reports and ensures lessons learned are used to improve processes.<br>• Reports on the organisation's overall compliance with this policy to the AI policy owner and governance committee. |
| **AI governance committee / authority** | Designated committee or authority responsible for expert consultation and oversight. | • Provides consultation for AI use cases that are flagged by the screening process.<br>• Acts as the escalation point for reviewing prohibited use cases or other policy disputes.<br>• Reviews and approves high-risk AI systems before deployment. |

| Role | Definition | Responsibilities |
|---|---|---|
| **AI system owner** | This is the person accountable for a specific AI system, its entire lifecycle, and its compliance with this policy. | • Accountable for ensuring their assigned AI systems comply with this policy, including risk assessments, approvals, and documentation. |
| **All employees and volunteers** | All employees, contractors, and other personnel covered by the scope of this policy. | • Adhere to the principles and statements outlined in this policy.<br>• Complete any required AI training to understand the capabilities, limitations and risks of the AI systems they use.<br>• Report any AI-related incidents, hazards or unexpected behaviour through the established channels. |

# New AI use case procedures

**Editing suggestion:** Every AI use case may represent new risks. You should document how your organisation will assess these use cases before moving forward. You can use the screening tool to help with this.

## Example text

All proposed AI use cases must be screened to identify and flag those that require enhanced governance or pose an unacceptable risk.

This screening process classifies each use case, resulting in an outcome (e.g., normal, elevated, prohibited) that determines the required level of risk assessment, oversight and approval. This ensures our governance effort is always proportionate to the potential impact of the AI system.

# Incident management

**Editing suggestion:** update this section to outline your approach to managing AI incidents. It should be integrated with your organisation's existing overall incident management framework.

## Example text

Any breaches or incidents involving AI must be reported to the **system owner and/or the compliance monitor** and managed in accordance with our organisation's incident response procedures.

Our organisation will ensure the capacity to take AI systems offline when necessary and will maintain documented manual processes as a fallback to ensure continuity of operations.

# Policy review

> A defined review cycle is essential for keeping your policy relevant. This is particularly important for AI use, as the technology is developing quickly.

**Editing suggestion:** customise the frequency and review triggers based on your organisation's context and the pace of change in the AI technologies you use.

## Example text

This policy will be reviewed **annually**, followed by a formal approval process, to ensure it remains current and effective.

An ad-hoc review may also be triggered by:

- a significant AI-related incident
- the emergence of new, impactful AI technologies
- changes to relevant laws, regulations, or industry standards.

The review process will be led by the AI policy owner in consultation with the AI governance committee**.** All substantive changes require formal approval from the policy approvers**.**

# Appendix

**Editing suggestion:** customise the glossary with terms relevant to your organisation and update the list of related documents to point to your specific internal policies and frameworks.

## Example text

We have provided the following Australian Government resources as supporting references. They do not form part of the formal policy. They may help you understand the broader context of AI governance and terminology.

- AI register template
- AI screening tool
- Australia's AI Ethics Principles
- Voluntary AI Safety Standard
- Glossary of Terms and Definitions