TheCyberGuyAU
Smarter Cyber. Safer Business.

Free AI Policy Template for Businesses

This resource should help businesses implement a basic AI policy aligned with Australian best practices.

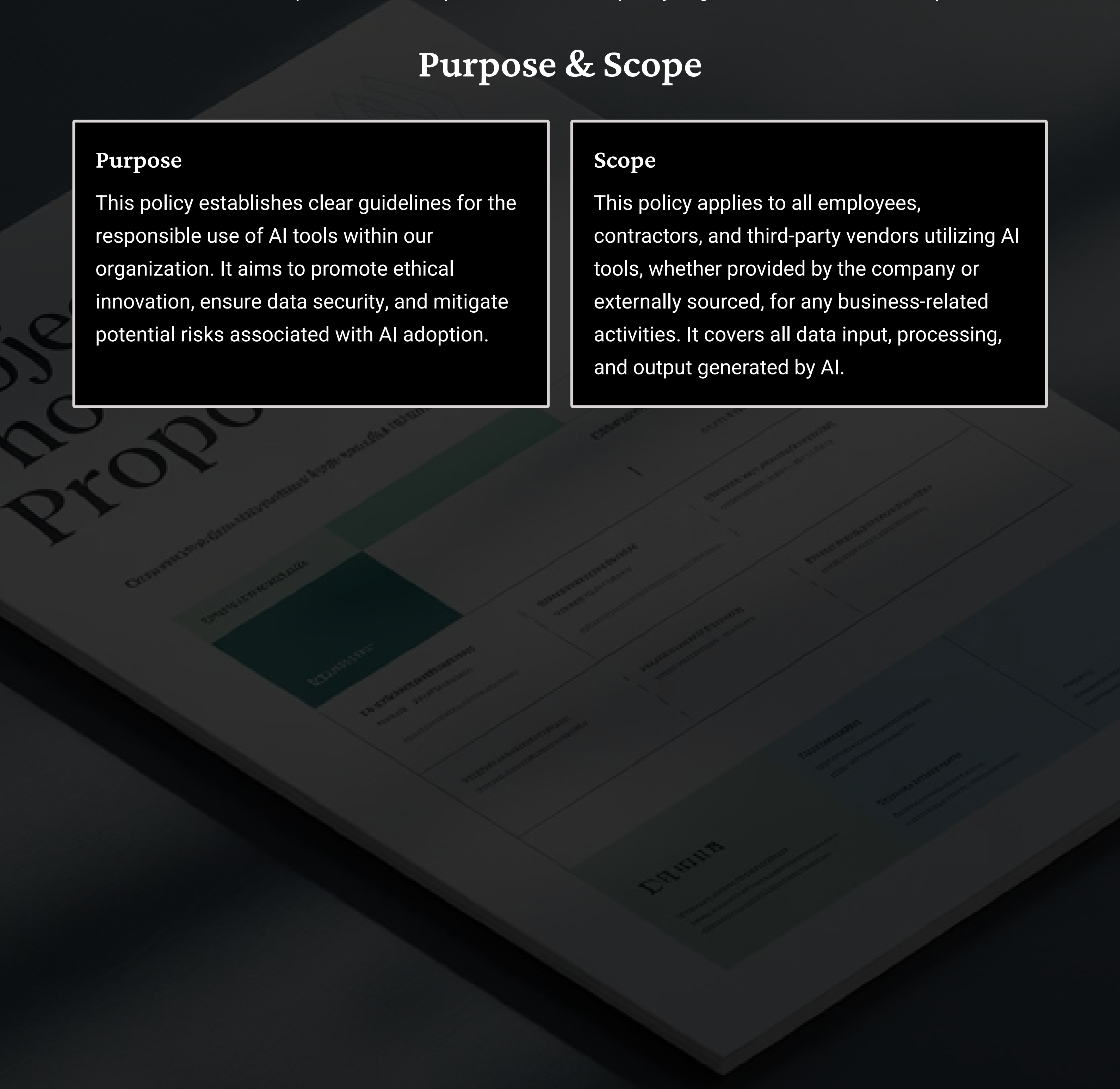
Purpose & Scope

Purpose

This policy establishes clear guidelines for the responsible use of AI tools within our organization. It aims to promote ethical innovation, ensure data security, and mitigate potential risks associated with AI adoption.

Scope

This policy applies to all employees, contractors, and third-party vendors utilizing AI tools, whether provided by the company or externally sourced, for any business-related activities. It covers all data input, processing, and output generated by AI.



1. Purpose & Scope

Policy Objectives

This policy clearly outlines our organization's objectives for implementing AI, ensuring responsible and ethical use.

Covered Parties

It applies to all employees, contractors, and third-party vendors involved in AI-related activities.

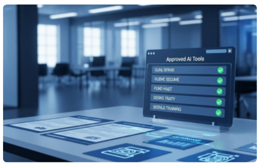
Defined Boundaries

This policy establishes the precise boundaries and scope of AI tool application within our operations.

2. Approved AI Tools

Tool Selection Process

- Security assessment requirements
- Privacy compliance verification
- Business need justification
- Cost-benefit analysis



Approved Tool List

Maintain a current list of organization-approved AI tools with details on:

- Tool name and version
- Approved use cases
- Required training
- Licensing information

3. Who Can Use AI Tools

Role-Based Access

Define which roles or positions are authorized to use specific AI tools based on job requirements and departmental needs, ensuring access is aligned with business functions.

Required Training

Specify any mandatory training programs or certification requirements employees must complete before being granted access to and using AI tools, covering ethical use and data handling.

Approval Process

Document the clear, step-by-step process for requesting access to new or existing AI tools, including necessary managerial and IT approvals, and criteria for expedited access.

3. AI Tool Usage and Data Guidelines

This section outlines who is authorized to use AI tools within the organization and the critical guidelines for data input to ensure security and compliance.

Data Input Guidelines

Sensitive Data Restrictions

Clearly define what types of data should never be input into AI tools, such as personal information, confidential business data, or proprietary information.

Data Verification

Establish processes for verifying the accuracy and appropriateness of data before it is used with AI tools.

Documentation Requirements

Outline any documentation needed when inputting data into AI systems, including data source tracking.

5. Output Handling & Storage

Output Verification

Establish procedures for reviewing and validating AI-generated outputs before use.

Storage Requirements

Define how AI-generated content should be stored, including:

- Required metadata and attribution
- Retention periods
- Security classifications
- Access controls

Sharing Protocols

Outline when and how AI-generated content can be shared internally and externally.

6. Prohibited Use Cases

Legal Compliance

Prohibit any AI use that violates applicable laws, regulations, or industry standards.

Ethical Boundaries

Forbid using AI for deceptive, discriminatory, or harmful purposes.

Business Restrictions

Specify any business-specific prohibited uses, such as automated decision-making in sensitive areas.

Bypassing Controls

Prohibit using AI to circumvent established security controls or approval processes.

7. Basic Risk & Compliance Notes

Users must be aware of inherent risks when using AI and ensure all activities comply with regulatory and internal standards. Key considerations include:

- **Intellectual Property & Confidentiality:** Recognize that AI output may not be company IP. Never input sensitive, confidential, or proprietary company data into public AI tools unless explicitly approved.
- **Data Privacy:** Adhere strictly to all data privacy regulations (e.g., GDPR, CCPA) when handling personal or sensitive information with AI systems.
- **Accuracy & Bias:** Always verify the accuracy of AI-generated content and be mindful of potential biases in outputs. AI models can hallucinate or produce inaccurate information.
- **Transparency & Auditability:** Document AI tool usage, inputs, and outputs as required to maintain an auditable trail for compliance purposes.
- **Continuous Training:** Stay informed about the evolving landscape of AI risks, best practices, and policy updates through ongoing training and awareness programs.

Document Owner: TheCyberGuyAU | Classification: Public Template | Version: 1.0 | Review Date: 12 months from implementation

7. Basic Risk & Compliance Notes

Legal Considerations

Highlight key legal requirements relevant to AI use in your jurisdiction, including privacy laws and industry regulations.

Risk Assessment

Outline a basic process for assessing risks associated with AI use, including accuracy, bias, and security concerns.

Documentation

Specify what documentation should be maintained regarding AI use, including decision logs and impact assessments.

8. Monitoring & Reporting Expectations

Ongoing Monitoring

Establish processes for regularly reviewing AI tool usage, including:

- Usage patterns and volumes
- Compliance with policy guidelines
- Effectiveness and business value
- Emerging risks or concerns

Incident Reporting

Define procedures for reporting policy violations or concerns, including:

- Reporting channels and contacts
- Required information
- Response timeframes
- Investigation process

9. Policy Review Cycle

Regular Review Process

Establish a schedule and process for reviewing and updating this policy, including:

- Review frequency (recommended annually)
- Responsible parties
- Approval requirements
- Version control procedures

10. Acknowledgement Section

Employee Acknowledgement

Include a section for employees to acknowledge they have read and understood the policy.

Employee Name: ______________________________

Employee Signature: _________________________

Date: ____

Manager Signature: ________________

Document Owner: TheCyberGuyAU | Classification: Public Template | Version: 1.0 | Review Date: 12 months from implementation

Want a Complete AI Governance Toolkit?

This template provides a basic starting point for your AI policy needs. For a comprehensive solution that includes detailed guidance, advanced templates, implementation tools, and expert support, upgrade to our full version.

Detailed Guidance

In-depth insights and best practices to navigate complex AI governance challenges.

Advanced Templates

Ready-to-use documents for various AI policies, risk assessments, and compliance needs.

Implementation Tools

Practical resources to help you deploy and manage your AI governance framework efficiently.

Expert Support

Access to specialists for personalized advice and troubleshooting.

Get the Full AI Governance Toolkit →