Australian Government
Department of Employment and Workplace Relations

Third-Party AI Assessment Application Form

Introduction

The Third-Party AI Assessment Application Form (the Form) is for organisations using Artificial Intelligence (AI) to deliver services for the Department of Employment and Workplace Relations (the Department). It ensures AI use is:

- Safe and responsible
- Protective of personal data
- Fair and respectful
- Aligned with human rights and Indigenous data sovereignty
- Human-centred in decision-making

When to Use the Form

The Form is used to help your organisation explain to us: why an AI system is required, how it will be used, and show how it meets the Department's expectations for ethics and cybersecurity.

You must complete the Form if:

- the AI system will be used to deliver services for the Department, or
- the AI system is not directly related to service delivery but cannot be fully isolated.

You do not need to complete the Form if:

- the AI system is only used for internal business tasks and can be fully isolated from service delivery conducted on behalf of the Department and all associated data.

How to Complete and Submit the Form

Before you start, read the Third-Party AI Assessment Framework (the Framework).

Each AI use case needs a separate form and written approval from the Department before it can be used.

Submit the completed form and supporting documents to securitycompliancesupport@dewr.gov.au

On receiving the Form, the Department will:

- Review your submission
- Request more information from your organisation as required
- Notify you of the outcome.

Contact us: securitycompliancesupport@dewr.gov.au

Table of Contents

Before You Submit the Form

Before submitting your application, please make sure you have completed the following internal checks.

Note: You do not need to include this checklist with your application. It is provided to help your organisation confirm readiness and alignment with Departmental expectations.

1. Relevance to Departmental Service Delivery

☐ Confirm the AI use case is directly related to delivering services on behalf of the Department. *If checked, proceed to Security Compliance below.*

☐ If it is not, confirm whether you can fully isolate the AI system from the delivery of services on the behalf of the Department. *If checked, you do not need to proceed with this form.*

2. Security Compliance

☐ Confirm that the AI technology is not listed under the Department of Home Affairs Protective Security Directions. *If it is listed as prohibited, the AI system must not be used.*

3. Internal Review and Endorsement

☐ An ethics review of the AI use case has been conducted by your organisation. *(Recommended)*

☐ A cybersecurity threat and risk assessment of the AI system has been conducted by your organisation. *(Recommended)*

Section 1: Organisation Details

This section collects key information about your organisation to assist the Department in matching the information with existing records, linking relevant contracts, and identifying appropriate contacts. It includes your organisation's name, business number, four-digit code (if known), contract list, and contact details.

Q1.1 Organisation details

Trading name	Click or tap here to enter text.
Legal name of organisation	Click or tap here to enter text.
***Australian Business Number (ABN) or Australian Company Number (*ACN**)**	Click or tap here to enter text.
Four-digit organisation code (if known)[1]	Click or tap here to enter text.
Contact email	Click or tap here to enter text.

[1]The four-digit code is the short identification (ID) that helps the Department understand which organisation you are from. It links your organisation to its contracts, services, and reports.

Q1.2 Deeds or Contracts

List the Deeds or Contracts your organisation holds with the Department. If there are more than one, list each separately.
Click or tap here to enter text.

Q1.3 Application contact officer

Please tell us who is leading your organisation's work with AI.

Name of AI lead	Click or tap here to enter text.
Position title	Click or tap here to enter text.
Email	Click or tap here to enter text.
Contact phone number	Click or tap here to enter text.
Delegated contact officer (if different)	Click or tap here to enter text.

Section 2: AI Use Case

This section captures details about your organisations' AI project so the Department can understand what it is, who made it, how it works, and whether it uses sensitive data or helps deliver services. It includes the AI system's name, development stage, who built it, what problems it solves, who it affects, and whether staff receive relevant training.

If your organisation already has a written AI plan, you can attach the plan instead of completing this section.

Q2.1	**What is the name of the AI system?**	Click or tap here to enter text.
Q2.2	**Which stage of the AI lifecycle best describes your use case?**	Choose an item.
Q2.3	**Will you be using an AI system developed by a Third-Party?**	Choose an item.
Q2.4	**Will your organisation develop the AI system in-house?**	Choose an item.
Q2.5	**Describe the AI use case.**	
Click or tap here to enter text. Prompts to help guide content: • the problem it aims to solve • the expected benefits and goals • who may be affected by the use of this AI solution		
Q2.6	**Will the AI system be used to deliver services on behalf of the Department?**	Choose an item.
Q2.7	**Will the AI system handle personal and/or sensitive information?**	Choose an item.
Q2.8	**Will the data be used for training or evaluating an AI model?**	Choose an item.
Q2.9	**Will any AI-related training be delivered to staff?**	Choose an item.

Section 3: Privacy protection and security

This section captures information around how your organisation keeps personal data safe when using AI, including what rules it follows, how it manages Third-Party systems, whether privacy risks have been checked, and if staff can access training; it covers standards, contracts, risk assessments, data protection methods, and secure data handling.

Q3.1	**What standards does your organisation follow when handling personal and sensitive information in relation to AI use?**	
Click or tap here to enter text. This should include how your organisation ensures compliance when collecting, storing, processing, and sharing such data.		
Q3.2	**If your organisation handles protected information under social security law, how does your organisation ensure compliance in relation to AI use?**	
Click or tap here to enter text. This could include how your organisation applies social security law to your AI use case through access controls, audits, and data governance.		
Q3.3	**If your organisation uses third-party AI systems or components, how are privacy obligations reflected and used in those systems?**	
Click or tap here to enter text. Explain how contracts, policies, or oversight help to manage this.		
Q3.4	**Has your organisation assessed privacy risks related to the AI system (e.g. through a Privacy Threshold Assessment or Privacy Impact Assessment)?**	Choose an item.
Q3.5	**Are privacy-preserving techniques (e.g. data minimisation, anonymisation, encryption) used?**	Choose an item.
Q3.6	**Are data lifecycle practices in place (e.g. secure backups and deletion) to protect stored information?**	Choose an item.
Q3.7	**Is mandatory privacy-related training provided to staff?**	Choose an item.

Section 4: Reliability and Safety

This section captures information about how your organisation keeps AI systems safe and working properly, including checking data quality, managing risks, tracking performance, using feedback, and making sure people can assist when required. It covers data checks, monitoring plans, safety controls, and human oversight.

Q4.1	**Does your organisation check that the data used in the AI system is suitable and relevant for its purpose?**	Choose an item.
Q4.2	**Are there controls in place to keep the data accurate, reliable, and high quality throughout the AI system's lifecycle?**	Choose an item.
If yes, briefly describe the key risks identified and how they are being managed:		
Q4.3	**Has your organisation established a plan to monitor how the AI system performs, including any measures or indicators used to assess its effectiveness?**	Choose an item.
Q4.4	**Is feedback from stakeholders used to improve the system?**	Choose an item.
Q4.5	**Are there procedures that allow people to step in and take control of the AI system when required?**	Choose an item.
Q4.6	**Can the AI system be paused, overridden, or turned off if risks or concerns arise?**	Choose an item.
If yes, briefly describe how human oversight is maintained and how ethical concerns are addressed in real time:		

Section 5: Human-Centred Values and Fairness

This section captures information about how your organisation ensures its AI system is fair and respectful to all people, including whether diverse voices were involved, if advice was taken from legal or ethics experts, and how fairness risks such as bias or harm are found and managed. It covers fairness goals, data checks, expert input, and how different groups are considered.

Q5.1	**Were people with diverse backgrounds, skills, or experiences involved in designing, building, or reviewing the AI system?**	Choose an item.
Q5.2	**Will the AI system use data about specific communities or population groups, including First Nations people or other groups with unique data sensitivities?**	Choose an item.
Q5.3	**Did your organisation get advice from legal or ethics experts to make sure the AI use case respects human rights?**	Choose an item.
Q5.4	**Has your organisation identified any potential negative or unintended consequences from the AI system?**	Choose an item.
If yes, briefly describe the risks and how they are being mitigated:		
Q5.5	**Does your organisation define what a fair outcome looks like for this AI use case?**	Choose an item.
Q5.6	**Is fairness measured using numbers or data (e.g. comparing results across different groups)?**	Choose an item.
Q5.7	**Is fairness assessed using feedback or expert review (e.g. stakeholder input, ethical advice)?**	Choose an item.
Q5.8	**Has your organisation found any fairness risks in the data (e.g. bias, missing representation, lack of consent)?**	Choose an item.
If yes, briefly describe how these risks are being addressed:		

Section 6: Contestability and Accountability

This section captures information about how your organisation ensures people are aware of when AI is used, can challenge decisions it influences, and are protected from ethical risks. It covers transparency, complaints processes, decision reviews, ethical concerns, and whether your organisation has policies or checks in place to support responsible AI use.

Q6.1	**Are people told when an AI system is used and may affect decisions about them?**	Choose an item.
Q6.2	**Is there a process to let people know when an AI system has a strong influence on an administrative decision?**	Choose an item.
Q6.3	**Does your organisation have a way to handle complaints or challenges about AI use?**	Choose an item.
Q6.4	**Is there a clear and timely way for people to challenge decisions made or influenced by AI?**	Choose an item.
If yes, briefly describe how people are informed and how they can challenge decisions:		
Q6.5	**Has your organisation identified any ethical risks linked to the AI system (e.g. limited explainability, low human oversight, privacy or psychological harm)?**	Choose an item.
If yes, briefly describe the risks and how they are being mitigated:		
Q6.6	**Has your organisation created an AI policy or framework to support responsible use?**	Choose an item.
Q6.7	**Has your organisation looked at supply chain risks related to the AI system?**	Choose an item.

Section 7: Transparency and Explainability

This section captures information about how your organisation ensures its AI system is clear and easy to understand, including whether communities were consulted, if information is shared publicly, if records are kept, and if people are told when AI is used. It also checks whether the system can explain its decisions and how data risks such as bias or poor quality are managed.

Q7.1	**Were people from relevant communities or groups consulted during the design or use of the AI system?**	Choose an item.
Q7.2	**Will your organisation share information about the AI system (e.g. its purpose, goals, methods, model, or outputs) with the public?**	Choose an item.
Q7.3	**Will your organisation keep records and documentation throughout the AI system's lifecycle?**	Choose an item.
Q7.4	**Are people told when they are interacting with or relying on an AI system?**	Choose an item.
Q7.5	**Can the AI system give clear explanations for its decisions, recommendations, or insights?**	Choose an item.
If yes, briefly describe how transparency and explainability are supported in practice:		
Q7.6	**Has your organisation identified any data-related risks in the AI system (e.g. bias, poor data quality, lack of consent, or linking data for the first time)?**	Choose an item.
If yes, briefly describe the risks and how they are being mitigated:		

Section 8: Cybersecurity

This section supports the evaluation of your organisation's security readiness when procuring or developing an AI system, particularly those based on using third-party Large Language Models (LLMs) and Application Programming Interfaces (APIs). The questions focus on identifying how well AI security is integrated into your existing Information Security Management System (ISMS) and broader risk management practices. They reflect key mitigation considerations outlined in the Australian Signals Directorate (ASD) guidelines on the governance and use of AI[1]. Your responses, in conjunction with previous sections, will help determine whether appropriate guardrails are in place to support the secure and responsible AI adoption by your organisation.

If you have an architecture design document and diagram, you can attach this to the Form.

Q8.1	**Is there a senior executive or appointed delegate responsible for overseeing AI security in your organisation?**	Choose an item.
Q8.2	**Is AI security integrated into your organisation's ISMS and risk management framework?**	Choose an item.
Briefly describe how your ISMS supports AI system security:		
Q8.3	**Have you documented security requirements of confidentiality, integrity and availability for the AI system?**	Choose an item.
Briefly describe the security requirements:		
Q8.4	**Is all data in the AI system processed and stored exclusively in Australia?**	Choose an item.
Briefly describe all relevant data types and their residency:		

[1] Artificial intelligence | Cyber.gov.au

Q8.5	**Do you have a clear understanding of the shared security responsibilities between your organisation and any third-party vendor of the AI system or components?**	Choose an item.
Q8.6	**Can you integrate the AI system with your organisation's cybersecurity tools, for example, firewalls, vulnerability scanner, incident detection and response tools, centralised logging and monitoring facilities?**	Choose an item.
Q8.7	**Is there contractual arrangement with the vendor about how your data is used, retained and disposed securely?**	Choose an item.
Briefly describe the contractual arrangement:		
Q8.8	**Do you have suitably qualified and adequately resourced employees to ensure the AI system is set-up, maintained and used securely?**	Choose an item.

Glossary

Term	Definition
AI Accountable Officer	An AI Accountable Officer is the senior individual within an organisation who holds strategic responsibility for the oversight and governance of AI initiatives. This role serves as the central point of coordination for AI-related activities, ensuring that the organisation's use of AI aligns with its values, objectives, and risk appetite.
Artificial Intelligence (AI)	As defined in the *Policy for the Responsible Use of AI in Government*, 'AI Technologies' means a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments and may vary in their levels of autonomy and adaptiveness after deployment.
Data Sovereignty	Data sovereignty refers to the right of a nation to control and manage its own data, regardless of where that data originated and [is] stored. This means that a country has the authority to determine how its data is collected, processed, and shared, as well as enforce its own laws and regulations related to data protection and privacy. Data sovereignty is often linked to national security, as countries may be concerned about foreign access to sensitive data.
Information Security Manual (ISM)	The Australian Signals Directorate produces the Information Security Manual (ISM). The ISM is a cybersecurity framework that an organisation can apply, using their risk management framework, to protect their information technology and operational technology systems, applications and data from cyberthreats.
Personal Information	The Privacy Act defines 'personal information' as: 'Information or an opinion about an identified individual, or an individual who is reasonably identifiable: a. whether the information or opinion is true or not; and b. whether the information or opinion is recorded in a material form or not.

Right Fit for Risk (RFFR) accreditation	The Department uses the External Systems Accreditation Framework (ESAF) and the Right Fit for Risk (RFFR) assurance approach to assess and accredit Providers' Information Security Management Systems (ISMS). The ESAF aligns with the Protective Security Policy Framework (PSPF) and supports the Department's accountability for safeguarding data across all contracted programs and systems.
Secure-by-Design	Secure by Design is a proactive, security-focused approach to the design, development and deployment of products and services that necessitates a holistic organisational approach to cybersecurity. For further information, refer to the Australian Signals Directorate Secure by Design guidance.
Sensitive information	Sensitive information is personal information that includes information or an opinion about an individual's: • racial or ethnic origin • political opinions or associations • religious or philosophical beliefs • trade union membership or associations • sexual orientation or practices • criminal record • health or genetic information • biometric information (some aspects). Generally, sensitive information has a higher level of privacy protection than other personal information.
Third-Party Organisation	Any external entity contracted by the Department to deliver services under a deed or contract or agreement. These organisations may include employment services providers, skills and training program providers, or other service delivery partners.