



~~OFFICIAL: Sensitive~~

Generative Artificial Intelligence Use Request

Use of generative Artificial Intelligence (AI) products by Department and ABF staff is governed to minimise risks of data breaches and other high-risk incidents that can lead to reputational damage, reduce trust, loss of access, and expose Department to legal action, liability, fines and compensation.

Use of generative AI products will only be provided to staff in business areas that have an approved Artificial Intelligence Risk Management Plan (AI-RMP) in place. The AI-RMP is a formal document that needs to be cleared by the requesting business area's SES Band 2, the Chief Information Security Officer (CISO) and the Chief Data Officer (CDO). An AI-RMP details the risks of use of the generative AI product by the business area and the controls that are in place to mitigate these risks. The implementation of these controls may be subject to monitoring and compliance audits.

An approved AI-RMP enables the business area's staff to request access to specific generative AI products, which are by default blocked on Home Affairs networks. Staff will not be granted access unless they are covered by an approved AI-RMP.

Please note: Use cases which currently pose an unacceptable risk include, but are not limited to:

- cases requiring input of:
 - large amounts of government data
 - classified, sensitive or confidential information
- cases where services will be delivered, or decisions will be made
- cases where coding outputs will be used in government systems.

Support

Additional support on the generative AI risk management plan can be sought from the Data Management and Ethics section within the Data and Economic Analysis Centre (DEAC):

s. 47E(d) [@homeaffairs.gov.au](mailto:s.47E(d)@homeaffairs.gov.au)

The AI-RMP process

You will need

- The official name of the generative AI product(s) being sought access to.
- The URL of the generative AI product (for web-based / web-accessible generative AI products)

The process

1. Complete this template and seek approval from the requesting business area's SES Band 2.
2. Submit the completed template to s. 47E(d) [@homeaffairs.gov.au](mailto:s.47E(d)@homeaffairs.gov.au)
3. DEAC (Data Management & Ethics Section) will then facilitate review and approval by the CDO and the CISO.
4. The AI-RMP will become active once approved by the requesting area's SES Band 2, the CDO and the CISO. The requesting business area's staff will then be able to apply for access to the specific AI products covered in this AI-RMP using Connected Services.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

~~OFFICIAL: Sensitive~~

~~OFFICIAL: Sensitive~~

About the requesting business area / business use

Requesting Business area details	
Requesting Division or Branch	ABF Commissioner Office
Staff details who are covered under this business case	ABF Commissioner, s. 47F(1) No other officer will have access under this request
Name of the generative AI product(s)	ChatGPT
URL or address of the generative AI product(s)	https://chat.openai.com (Mobile App)
Describe how the generative AI product(s) will be used	ChatGPT will be used via mobile application – primarily using the query and search functions to generate narrative responses.
Describe the purpose for using the generative AI product(s)	s. 47E(d)
Impact if use of the generative AI product(s) is not approved	
SES Band 2 (Accountable Risk Owner)	Christie Sawczuk – Assistant Commissioner, Strategy and Governance

Released by Department of Home Affairs
under the Freedom of Information Act 1982

~~OFFICIAL: Sensitive~~

~~OFFICIAL: Sensitive~~**Business Area SES Band 2:**

- ☒ I confirm that the proposal above is consistent with the interim guidance for government use of generative AI.
- ☒ I note the risks, controls, and treatments identified above in Parts A, B and C.
- ☐ I acknowledge that I am accountable for ensuring all of the identified risks – and any subsequently identified risks – relating to the use of the generative AI product are managed in accordance with the Department's risk management framework.
- ☒ I confirm that these risks will be continuously monitored and reviewed, and will also be reported on as required through quarterly business plan reporting and under the Department's risk management framework.

s. 47F(1)

Name: s. 47F(1)

Signature:

Date: 12.3.24

Chief Data Officer

- ☒ I agree that this proposal is consistent with the interim guidance for government use of generative AI.
- ☒ I agree that the controls identified above in Part B will effectively support adherence to current AI Use Ethical Principles.

Name: s. 47F(1)

Signature:

s. 47F(1)

Date: 12.3.24

Chief Information Security Officer

- ☐ I agree that this proposal is consistent with the interim guidance for government use of generative AI.
- ☐ I note the Information Security risks identified in Part A above, and agree that the controls (and, where appropriate, treatments) set out in Parts A and C should ensure they are effectively managed within the Department's risk appetite.

Name:

Signature:

Date:

~~OFFICIAL: Sensitive~~



OFFICIAL

Minute

To: Chief Operating Officer

Cc: Chief Data Officer

Date: 15 March 2024

Reference: s. 22(1)(a)(ii)

Generative Artificial Intelligence Use Request

Timing

At your convenience.

Purpose

To:

1. **Note** the attached Home Affairs Artificial Intelligence (AI) Product Use Risk Management Plan (Attachment A); and
2. **Seek approval** for the acting Group Manager Technology and Major Capability Group (TMCG), s. 47F(1) to access ChatGPT from Departmental devices.

Background

3. Use of Generative AI products by Department and ABF staff is governed to minimise risks of data breaches and other high-risk incidents.
4. For staff to access Generative AI products, a Risk Management Plan must be put in place and approved by the staff member's SES Band 3, the Chief Data Officer and the Chief Information Security Officer.

s. 22(1)(a)(ii)

6. It is important for the Department to be on the front foot when it comes to using Generative AI to ensure we are seen as an agency that is taking action to investigate the uses and benefits of the tool within our processes and workplace.

s. 47E(d)

OFFICIAL

OFFICIAL

s. 47E(d)

Consultation

- Consultation was not undertaken for this minute as the request is only intended to provide the Group Manager TMCG with access to ChatGPT.

Recommendation

It is recommended that you:

Note the attached Home Affairs AI Product User Risk Management Plan at Attachment A.

Noted

Approve the acting Group Manager Technology and Major Capability Group, s. 47F(1) to access ChatGPT from Departmental devices.

Approved

s. 22(1)(a)(ii)

Matt Jones
A/g Chief Information Officer
s 11C(1)(a)
14 March 2024

s. 22(1)(a)(ii)

Charlotte Tressler
Chief Operating Officer
March 2024
S. 11C(1)(a)

Contact Officer: s. 22(1)(a)(ii)

Division/Branch: ICT Division

Phone: s. 22(1)(a)(ii)

Attachment:

A. Home Affairs AI Product Use Risk Management Plan

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL



~~OFFICIAL: Sensitive~~

Generative Artificial Intelligence Use Request

Use of generative Artificial Intelligence (AI) products by Department and ABF staff is governed to minimise risks of data breaches and other high-risk incidents that can lead to reputational damage, reduce trust, loss of access, and expose Department to legal action, liability, fines and compensation.

Use of generative AI products will only be provided to staff in business areas that have an approved Artificial Intelligence Risk Management Plan (AI-RMP) in place. The AI-RMP is a formal document that needs to be cleared by the requesting business area's SES Band 2, the Chief Information Security Officer (CISO) and the Chief Data Officer (CDO). An AI-RMP details the risks of use of the generative AI product by the business area and the controls that are in place to mitigate these risks. The implementation of these controls may be subject to monitoring and compliance audits.

An approved AI-RMP enables the business area's staff to request access to specific generative AI products, which are by default blocked on Home Affairs networks. Staff will not be granted access unless they are covered by an approved AI-RMP.

Please note: Use cases which currently pose an unacceptable risk include, but are not limited to:

- cases requiring input of:
 - large amounts of government data
 - classified, sensitive or confidential information
- cases where services will be delivered, or decisions will be made
- cases where coding outputs will be used in government systems

Support

Additional support on the generative AI risk management plan can be sought from the Data Management and Ethics section within the Data and Economic Analysis Centre (DEAC): [s. 22\(1\)\(a\)\(ii\)@homeaffairs.gov.au](mailto:s.22(1)(a)(ii)@homeaffairs.gov.au)

The AI-RMP process

You will need

- The official name of the generative AI product(s) being sought access to.
- The URL of the generative AI product (for web-based / web-accessible generative AI products)

The process

1. Complete this template and seek approval from the requesting business area's SES Band 2.
2. Submit the completed template to [s. 22\(1\)\(a\)\(ii\)@homeaffairs.gov.au](mailto:s.22(1)(a)(ii)@homeaffairs.gov.au)
3. DEAC (Data Management & Ethics Section) will then facilitate review and approval by the CDO and the CISO.
4. The AI-RMP will become active once approved by the requesting area's SES Band 2, the CDO and the CISO. The requesting business area's staff will then be able to apply for access to the specific AI products covered in this AI-RMP using Connected Services.

~~OFFICIAL: Sensitive~~

~~OFFICIAL: Sensitive~~

About the requesting business area / business use

Requesting Business area details	
Requesting Division or Branch	Technology and Major Capability Group
Staff details who are covered under this business case	s. 47F(1)
Name of the generative AI product(s)	ChatGPT
URL or address of the generative AI product(s)	https://chat.openai.com
Describe how the generative AI product(s) will be used	s. 22(1)(a)(ii)
Describe the purpose for using the generative AI product(s)	
Impact if use of the generative AI product(s) is not approved	
SES Band 2 (Accountable Risk Owner)	Charlotte Tressler, Deputy Secretary Chief Operating Officer Group

Released by Department of Home Affairs
under the *Freedom of Information Act 1982*

~~OFFICIAL: Sensitive~~

~~OFFICIAL: Sensitive~~**Business Area SES Band 3:**

☒ I confirm that the proposal above is consistent with the interim guidance for government use of generative AI.

☒ I note the risks, controls, and treatments identified above in Parts A, B and C.

☒ I acknowledge that I am accountable for ensuring all of the identified risks – and any subsequently identified risks – relating to the use of the generative AI product are managed in accordance with the Department's risk management framework.

☒ I confirm that these risks will be continuously monitored and reviewed, and will also be reported on as required through quarterly business plan reporting and under the Department's risk management framework.

Name: Charlotte Tressler

Signature:

s. 22(1)(a)(ii)

Date:

11/4/2024

Chief Data Officer

☒ I agree that this proposal is consistent with the interim guidance for government use of generative AI.

☒ I agree that the controls identified above in Part B will effectively support adherence to current AI Use Ethical Principles.

Name:

s. 47F(1)

Signature:

Date:

18.3.24

Chief Information Security Officer

☐ I agree that this proposal is consistent with the interim guidance for government use of generative AI.

☐ I note the Information Security risks identified in Part A above, and agree that the controls (and, where appropriate, treatments) set out in Parts A and C should ensure they are effectively managed within the Department's risk appetite.

Name:

Signature:

Date:

~~OFFICIAL: Sensitive~~



Australian Government
Department of Home Affairs

~~OFFICIAL: Sensitive~~

Generative Artificial Intelligence Use Risk Management Plan

Use of generative Artificial Intelligence (AI) products, such as ChatGPT and Bard, by Department and ABF staff is governed to minimise risks of data breaches and other high-risk incidents that can lead to reputational damage, reduce trust, and expose the Department to legal action, liability, fines and compensation.

Use of generative AI products will only be provided to staff in business areas that have an approved Artificial Intelligence Risk Management Plan (AI-RMP) in place. The AI-RMP is a formal document that needs to be cleared by the requesting business area's SES Band 2, the Chief Information Security Officer (CISO) and the Chief Data Officer (CDO). An AI-RMP details the risks of use of the generative AI product by the business area and the controls that are in place to mitigate these risks. The implementation of these controls may be subject to monitoring and compliance audits.

An approved AI-RMP enables staff to request access to specific generative AI products, which are by default blocked on Home Affairs networks. Staff will not be granted access unless they have an approved AI-RMP.

The AI-RMP process

You will need

- The official name of the generative AI product(s) that you require access to.
- The URL of the generative AI product (for web-based / web-accessible generative AI products).

The process

1. Complete this template and seek approval from your SES Band 2.
2. Submit the completed template to [s.22\(1\)\(a\)\(ii\)@homeaffairs.gov.au](mailto:s.22(1)(a)(ii)@homeaffairs.gov.au)
3. DEAC (Data Management & Ethics Section) will then facilitate review and approval by the CDO and the CISO.
4. The AI-RMP will become active once approved by your SES Band 2, the CDO and the CISO. Staff will then be able to apply for access to the specific AI products covered in this AI-RMP using Connected Services.

Please Note

This risk management plan provides coverage for all staff and purposes mentioned (below) as in scope. There is no need for an individual staff member to submit a risk management plan. This risk management plan would be submitted by the SES Band 2 of the requesting business area and approved by the Chief Data Officer (CDO) and Chief Information Security Officer (CISO).

~~OFFICIAL: Sensitive~~

~~OFFICIAL: Sensitive~~**Support**

Additional support pertaining to the generative AI risk management plan can be sought from Data and Economic Analysis Centre (DEAC), by Data Management and Ethics section contactable by email

Data Management and Ethics Section

Data, Economics and Analytics Centre

s. 22(1)(a)(ii) @homeaffairs.gov.au

AI Product Access Risk management plan Template

About the requesting business area

Requesting Business area details	
Requesting Division or Branch	NEMA – Crisis Analysis and Planning Section, NCOB
Staff details (e.g. roles) who are will use the generative AI product(s)	s. 22(1)(a)(ii)
Name of the generative AI product(s)	Azure OpenAI Service – Chat GPT 4.0 integration
URL or address of the generative AI product(s)	Azure OpenAI Service – Advanced Language Models Microsoft Azure
Describe how the generative AI product(s) will be used	s. 47E(d)
Describe the purpose(s) for using the generative AI product(s)	

Business Area SES Band 2:

☒ I accept the Business Risks risk assessment and identified controls.

☒ I am accountable for ensuring all of the identified controls, including monitoring, are in place and followed to mitigate risks of use of the generative AI product. *subject to those using and managing the AI capability have implemented controls to mitigate the risks identified.*

Name:

s. 47F(1)

s. 47F(1)

Date:

23/4/24

NEMA

Chief Data Officer

☒ I accept the identified controls will promote observance of current AI Use Ethical Principles.

Name:

s. 47F(1)

Signature:

s. 47F(1)

Date: 24 April 2024

NEMA

Chief Information Security Officer

☒ I accept the Information Security risk assessment and the identified controls.

Name:

SANDON MORRIS

Signature:

s. 22(1)(a)(ii)

Date:

30 Apr 24

~~OFFICIAL: Sensitive~~