



Australian Government

Department of the Prime Minister and Cabinet

OFFICIAL

# PM&C Artificial Intelligence (AI) Policy

Version 1.0.0. October 2024

Information Services Division



# Contents

|                                                                                                   |   |
|---------------------------------------------------------------------------------------------------|---|
| 1 Synopsis.....                                                                                   | 1 |
| 1.1 Document Description.....                                                                     | 1 |
| 2 Contact details.....                                                                            | 1 |
| 2.1 Document creation .....                                                                       | 1 |
| 2.2 Amendment, Review and Approval .....                                                          | 1 |
| 2.3 References.....                                                                               | 1 |
| 3 Introduction .....                                                                              | 2 |
| 3.1 OECD definition of AI .....                                                                   | 2 |
| 3.2 Scope .....                                                                                   | 2 |
| 3.3 Authority.....                                                                                | 3 |
| 3.4 Objectives.....                                                                               | 4 |
| 3.5 Purpose .....                                                                                 | 4 |
| 3.6 Non-approved systems for AI .....                                                             | 4 |
| 3.7 Minimum standards .....                                                                       | 5 |
| 3.8 Accreditation and authorisation of AI within PM&C .....                                       | 5 |
| 3.8.1 Approving authority .....                                                                   | 5 |
| 3.8.2 AI assessing authority .....                                                                | 5 |
| 3.8.3 AI security risk assessment .....                                                           | 6 |
| 3.8.4 Technical security risk assessment.....                                                     | 6 |
| 3.8.5 Operational security risk assessment.....                                                   | 6 |
| 3.8.6 Strategic security risk assessment .....                                                    | 6 |
| 3.8.7 Privacy and legal risk assessment .....                                                     | 6 |
| 3.9 Request for AI technology at PM&C .....                                                       | 6 |
| 3.10 Principles.....                                                                              | 7 |
| 3.11 Standards.....                                                                               | 8 |
| 4 Roles and responsibilities .....                                                                | 8 |
| 4.1 Agency Head .....                                                                             | 8 |
| 4.2 Chief Operating Officer (COO).....                                                            | 8 |
| 4.3 Chief Security Officer (CSO) / First Assistant Secretary, Information Services Division ..... | 9 |

|                                                                                            |                                     |
|--------------------------------------------------------------------------------------------|-------------------------------------|
| 4.5 Information Technology Security Adviser (ITSA).....                                    | 10                                  |
| 4.6 Managers.....                                                                          | 10                                  |
| 4.7 AI business owners.....                                                                | 10                                  |
| 4.8 AI technical owners.....                                                               | 11                                  |
| 4.9 Authorised user responsibilities – AI.....                                             | 11                                  |
| Summary of User Responsibilities .....                                                     | <b>Error! Bookmark not defined.</b> |
| 5 AI account management.....                                                               | 11                                  |
| 5.1 AI user account management principles / procurement .....                              | 11                                  |
| 5.2 Responsibilities – business owner .....                                                | 12                                  |
| 5.3 Responsibilities – ICT Procurement .....                                               | 12                                  |
| 5.4 User identification on AI platforms.....                                               | 12                                  |
| 5.5 Multi-Factor authentication – AI products / services on approval of AI .....           | 12                                  |
| 5.6 Passwords.....                                                                         | 13                                  |
| 5.6.1 Minimum AI password requirements .....                                               | 13                                  |
| 6 Personal use of AI technology on departmental assets .....                               | 13                                  |
| 6.1 Incidental personal use of AI on departmental assets .....                             | 13                                  |
| 6.2 Monitoring of personal use.....                                                        | 14                                  |
| 7 AI security incident reporting.....                                                      | 14                                  |
| 7.1 Reporting of an AI Technology - incident, breach, infringement, and/or violation ..... | 14                                  |
| 7.2 Appendix A – Australia’s 8 AI ethics principles .....                                  | 14                                  |

# 1 Synopsis

## 1.1 Document Description

This document details the Department of the Prime Minister and Cabinet (PM&C) policy with regards to the provision and use of Artificial Intelligence (AI) technology that must be adhered to when using PM&C Information Communication and Technology (ICT) systems to access AI technology.

## 2 Contact details

### 2.1 Document creation

| Author | Telephone | Email                                                |
|--------|-----------|------------------------------------------------------|
| ITSA   | s 47E(d)  | s 47E( <a href="mailto:pmc.gov.au">@pmc.gov.au</a> ) |

### 2.2 Amendment, Review and Approval

| Date     | Version | Comments        |
|----------|---------|-----------------|
| 17/10/24 | 1.0     | Initial release |

### 2.3 References

The following documents have been used as references in the preparation of this AI Policy.

| Reference                                                                                                 | Version | Owner                                       |
|-----------------------------------------------------------------------------------------------------------|---------|---------------------------------------------|
| <a href="#">National Framework for the assurance of artificial intelligence in Government - June 2024</a> |         | Australian, state and territory governments |
| <a href="#">Protective Security Policy Framework (PSPF)</a>                                               |         | Department of Home Affairs                  |
| The Australian Government Information Security Manual (ISM)                                               |         | Australian Cyber Security Centre            |

| Reference                                                                                            | Version | Owner                                               |
|------------------------------------------------------------------------------------------------------|---------|-----------------------------------------------------|
| NSW Govt. Artificial Intelligence Assurance Framework                                                |         | NSW Government                                      |
| NSW Govt. The NSW AI Assessment Framework                                                            |         | NSW Government                                      |
| UK National Cyber Security Centre (NCSC), US CISA, ASD - Guidelines for secure AI System Development |         | Australia, United Kingdom, United States of America |

## 3 Introduction

This policy has been developed to align with the Digital Transformation Agency's (DTA) interim guidance on government use of generative AI technologies for staff within Australian Government agencies.

AI describes a family of technologies that brings together computing power, scalability, networking, connected devices and interfaces, and data. AI technologies and systems built on these technologies can be programmed to perform specific tasks such as reasoning, planning, natural language processing, computer vision, audio processing, interaction, prediction and more. AI technologies can operate with varying levels of autonomy.

The desired outcome in [public sector adoption of AI](#) are as follows:

- increase confidence and reduce duplication in the adoption of AI technology in a public sector context
- provide a structure for consistent application of the technologies
- provide the guardrails to achieve efficiencies and reduce duplication.

In addition, as AI technology evolves, the legal and ethical provision and use of AI technology within PM&C will be a key consideration.

### 3.1 OECD definition of AI

The Organisation for Economic Co-operation and Development (OECD) approved the following definition of AI:

*"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. Different AI systems vary in their levels of autonomy and adaptiveness after deployment."*

### 3.2 Scope

This document details the scope of PM&C's AI policy and applies to the following:

- all PM&C APS employees, consultants and contractors
- all APS employees, consultants and contractors that use PM&C ICT systems under ICT shared service arrangements  
Prime Ministers' Office (PMO) and portfolio ministers' offices
- other persons and organisations, which have been given authorised access to PM&C ICT systems and information assets.

This policy details the following:

- principles for the use of AI technologies within PM&C
- considerations of the provision and use of AI technology within the PM&C ICT environment
- process for assessment and approval of AI technology for use in PM&C ICT environment
- governance and oversight of the use of AI technology within PM&C ICT environment.

### 3.3 Authority

This document has been reviewed and endorsed by First Assistant Secretary, Information Services Division, First Assistant Secretary, Corporate, Chief Security Officer (CSO) and Chief Information Officer (CIO).

This policy will be reviewed and updated annually and is the responsibility of the PM&C IT Security Team under the direction of the Director, Cyber Security.

An AI technology is deemed authorised for access, on a case by case basis, within the PM&C ICT environment when:

- the AI technology has undergone a cyber-security assessment
- the AI technology has undergone a legal and privacy assessment, to ensure that it does not breach PM&C's legal and privacy obligations (refer section 3.8.7)
- an Authority to Operate (ATO) Minute has been approved by the CSO / CIO and issued to the requesting Business Owner.

In authorising and accrediting an AI technology, requesters are to consider the following:

- what is the business need or requirement: to perform basic administrative functions, outline why the requested AI technology is the best means to achieve the business need or to speed up processing time. This needs to be stated as clearly as possible in the form of a benefit statement.
- is the AI technology, branch specific or could it be used agency wide: This is an important consideration as it will dictate what sort of AI technology licence / subscription is required.
- is this proposed AI technology a trial / proof of concept: Requesters are to provide statements whether this is a trial or proof of concept and what the expectations are?

### 3.4 Objectives

The objective of the PM&C AI policy is to:

- articulate the rules for the provision, use and deployment of AI technology within PM&C
- articulate the approaches and practices to protect PM&C from any adverse impact from the use of AI technology
- detail the process of assessment of the AI technology, for suitability, functionality, risk, and conditions of use within PM&C
- protect the confidentiality, security, availability and integrity of PM&C data and information.

The policy is presented in clear language to ensure PM&C users understand their obligations with regards to:

- requesting the use of an AI based technology
- protection of official information when considering the use of an AI technology.

### 3.5 Purpose

This policy covers all aspects of the access, provision, deployment and use of AI technology, from and for the following PM&C systems:

- PM&C <sup>s 47E(d)</sup> [REDACTED]
- <sup>s 47E(d)</sup> [REDACTED]
- Shared services that PM&C provide: <sup>s 47E(d)</sup> [REDACTED]
- PM&C <sup>s 47E(d)</sup> [REDACTED]

This policy outlines the following key areas:

- AI technology security requirements for users of PM&C systems
- AI Security objectives
- correct use of AI technology within PM&C ICT environment
- secure use of AI (at least risk)
- security in the deployment of AI in PM&C.

### 3.6 Non-approved systems for AI

AI technologies **are not approved for and are not to be provisioned, deployed or used under any circumstances** on the following systems / networks:

<sup>s 47E(d)</sup> [REDACTED]

## 3.7 Minimum standards

All PM&C and shared services APS employees, consultants and contractors, **must adhere** to the minimum standards and rules, as defined in this policy as part of their employment responsibilities.

A policy control within this document with a '**must**' or '**must not**' requirement indicates that use, or non-use, of the control is mandatory.

Special dispensation / Approval **must be sought** from the **Chief Security Officer / Chief Information Officer (CSO/ CIO)** to deviate from a policy control outlined in this document that includes the term '**must**'.

Policies and standards are essential to support PM&C's business. The Department of the Prime Minister and Cabinet Security Framework contains details of the applicable legislation.

The use of AI technology must be lawful and align with legislation and policies relating to information and data, including, but not limited to, the [Privacy Act 1988](#), [Copyright Act 1968](#), and the [Protective Security Policy Framework](#). The DTA [Related Frameworks for AI](#) provides a further listing of frameworks that can be considered.

In addition, elements of this policy are drawn from the [APS Values and Code of Conduct](#) and PM&C's [Data Breach Response Plan \(DBR Plan\)](#).

## 3.8 Accreditation and authorisation of AI within PM&C

Security assessment, accreditation and authorisation for the use and operation of any AI technology within PM&C is the responsibility of the CSO, Director of Architecture, and the PM&C IT Security Team.

### 3.8.1 Approving authority

The CSO and CIO are the **Approving Authorities** for the provision, access to and use of AI technology within PM&C ICT environment. The approval or denial of the use of a specific AI technology will be based on the security risk assessment conducted by the PM&C IT Security Team and the level of risk that the use of that AI technology presents to the department.

### 3.8.2 AI assessing authority

The Director of Architecture Services and the Director Cyber Security are the **Assessing Authorities** for the provision, access and use of AI technology within PM&C ICT environment.

The **Director Architecture Services** is responsible for assessing the AI technology, to ensure that:

- it fits within the PM&C ICT environment
- meets the business need

- is aligned with PM&C's ICT strategy
- meets [Deploying AI Systems Securely | Cyber.gov.au](#)
- meets [Secure-by-Design | Cyber.gov.au](#).

The **Director Cyber Security** is responsible for the overall conduct of the cyber security risk assessment for the proposed AI technology, to ensure that the provision and use of that technology:

- the use of that AI technology presents an acceptable level of risk to PM&C ICT environment, information and people
- has sound mitigations and treatments in place to ensure the minimum likelihood of a data breach / spillage / compromise.

### 3.8.3 AI security risk assessment

The **PM&C IT Security Team** is responsible for conducting a cyber security risk assessment of any proposed AI technology. The risk assessment will assess the following:

### 3.8.4 Technical security risk assessment

- types and classification of information to be transmitted, processed, stored, and returned
- how information is transmitted, processed, and stored by the AI technology
- access to AI technology i.e. Account creation and management.

### 3.8.5 Operational security risk assessment

- business headquarters location / country of origin of the AI technology, product, or service
- hosted location / country of the proposed AI technology, platform, product, or service
- expected results from the AI technology.

### 3.8.6 Strategic security risk assessment

- legal and privacy considerations.

### 3.8.7 Privacy and legal risk assessment

Given the evolving nature of AI technology, it will be necessary to undertake a privacy and legal assessment. This must be obtained as part of the request process. Contact PM&C's Legal Policy Team via s 47E(d) [@pmc.go.au](mailto:s 47E(d)@pmc.go.au) or (s 47E(d)) and the PM&C Privacy Team via [privacy@pmc.gov.au](mailto:privacy@pmc.gov.au) or s 47E(d).

## 3.9 Request for AI technology at PM&C

Staff can request access through the [Service Portal](#) with a business case approved by their SES manager.

All requests/ proposals for access and use of an AI technology within PM&C are to undergo the following assessment:

|                        |                                                                                                                                                                                                                                                                                                                                    |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Request                | A request is to be raised using the 'Request Additional Software' form in the service portal                                                                                                                                                                                                                                       |
| IAC                    | An initial Architecture and Security Consideration (IAC) will occur with the requester; this will seek to understand the nature and scope of the request.                                                                                                                                                                          |
| Legal & Privacy        | Requesters are to obtain legal and privacy advice in relation to the request.                                                                                                                                                                                                                                                      |
| Assessment             | Conduct of the Security Risk Assessment of the proposed AI technology, platform, product or service with recommendations to authorise or not-to-proceed.                                                                                                                                                                           |
| ISD<br>CIO/FAS         | The First Assistant Secretary (FAS) within the Information Services Division (ISD) and the Chief Information Officer (CIO) will review findings and recommendations. The CIO will either approve or deny access to the AI technology. This will be achieved through an Authority to Operate Minute for the AI technology/platform. |
| Approval & Procurement | If approved to proceed, ICT Procurement is notified and conducts the procurement of the required AI technology.                                                                                                                                                                                                                    |

### 3.10 Principles

In addition to the [Australia's AI Ethics Principles](#), PM&C has adopted the following five **AI Principles for Use** which users are to always apply, when using authorised AI technologies within PM&C:

1. **AI is to be deployed responsibly** – Only AI tools that have been **authorised** for access and use within PM&C are to be deployed. Any responses from AI tools are to be reviewed for accuracy and biases.
2. **Transparency and explainability** – Users **must** critically examine AI outputs and ensure they can explain and justify their advice and decisions.
3. **Privacy protection and security** – AI input **must not** include or reveal classified, sensitive, or personal information. All activities related to AI technology must align with the *Privacy Act 1988*, which provides a specific definition of 'personal information' and 'sensitive information'.
4. **Accountability and human-centred decision-making** – Generative AI tools **must not** be the final decision-maker on government advice and services. Humans are the final decision-maker in the government process.

5. **Human, societal and environmental wellbeing** – Users are only to use authorised generative AI technology in a manner that is:
  - consistent with the APS Values, Employment Principles and Code of Conduct
  - consistent with the expectations of First Nations peoples, particularly around Indigenous data sovereignty and governance.

### 3.11 Standards

PM&C has adopted a “secure at all times” approach with regards to access, provision and use of AI in a PM&C environment. The following minimum standards apply to the application, deployment and use of AI technologies within PM&C ICT environments:

- **secure design** – including understanding risks and threat modelling
- **secure development** - development stage of the AI system development life cycle, including supply chain security, documentation, and asset and technical debt management
- **secure deployment of AI systems** – AI systems are deployed
- **secure operation and maintenance**
- **ethical use** – the use of AI technology **must** be line with Australia’s 8 AI Ethics Principles and the AI Principles of Use.

## 4 Roles and responsibilities

### 4.1 Agency Head

The Secretary provides support for the development, implementation and ongoing maintenance of information security processes and infrastructure. For day-to-day operations, the Secretary has delegated his authority to approve variations from requirements in this policy to the Chief Operating Officer (COO), Chief Security Officer (CSO) and Chief Information Officer (CIO) who is supported by the Information Technology Adviser (ITSA) and the PM&C Security Team.

### 4.2 Chief Operating Officer (COO)

The Deputy Secretary, government and corporate/COO is responsible for the day to day safe, legal, ethical and responsible use of AI technology within PM&C. This includes:

- governance and oversight of the PM&C AI policy
- oversight and overall compliance of the PM&C AI processes and procedures
- Ongoing oversight of the PM&C AI security, risk, and privacy assessment processes.

### 4.3 Chief Security Officer (CSO) / First Assistant Secretary, Information Services Division

The First Assistant Secretary of the Information Services Division (FAS, ISD) oversees the evaluation and implementation of AI technology within PM&C. The FAS, ISD collaborates with the Chief Security Officer (CSO) to address significant risks that require mitigation.

#### 4.3.1 CSO

The responsibilities of CSO includes:

- maintaining situational awareness of any updates and changes to legislation, regulations and policies as these apply to AI
- ensuring that Australia's AI Ethics Principles are applied in the development, deployment, management and use of any AI technologies within PM&C
- establishing monitoring and reporting systems and processes to measure performance and other issues relating to these technologies
- ongoing assurance on compliance and reporting including audit, risk and compliance of AI technologies
- managing and mitigation of high to extreme risks in conjunction with FAS ISD.

#### 4.3.2 FAS, ISD

The responsibilities of FAS, ISD includes:

- cyber security leadership and guidance for the provision and use of AI technologies within PM&C
- acting as the Approving Authority for the use of AI, based on the security risk assessment and advice
- ensuring that PM&C complies with legislation, regulations and policies as these apply to AI
- maintaining situational awareness of any updates and changes to legislation, regulations and policies as these apply to AI
- ensuring that Australia's AI Ethics Principles are applied in the development, deployment, management and use of any AI technologies within PM&C
- establishing monitoring and reporting systems and processes to measure performance and other issues relating to these technologies
- engaging with agencies with prior experience in adoption of these technologies to leverage existing investment as well as knowledge, patterns, and services.

### 4.4 Chief Information Officer (CIO)

The CIO is responsible for:

- ensuring that PM&C's AI technology practices comply with its obligations and responsibilities as an Australian Government agency

- acting as the Approving Authority for the use of AI technologies, based on the security risk assessment and advice
- acting as interdepartmental liaison for whole-of-government AI technology initiatives, such as implementing AI technology standards, information and system interoperability.

## 4.5 Information Technology Security Adviser (ITSA)

The Director Cyber Security, in their role as the Information Technology Security Adviser (ITSA) and the PM&C IT Security Team, are responsible for the conduct of security risk security management of AI technology, including security management across PM&C.

The ITSA's responsibilities include:

- provision of guidance and advice on all cyber security matters on AI technology including review and approve AI technology
- maintaining the currency and effectiveness of AI security policies, practices and procedures within PM&C
- initiating, conducting and/or participating in reviews and audits of the use of AI technology, products and services within PM&C
- analysing the security impact of AI related changes to the ICT environment
- acting on reported AI related security incidents
- engage with agencies with prior experience in adoption of AI technologies to leverage existing investment as well as knowledge, patterns, and services.

For issues relating to the secure provision and use of artificial intelligence, the ITSA can be contacted by calling S 47E(d) or via email at: S 47E [@pmc.gov.au](mailto:pmc.gov.au)

## 4.6 Managers

Managers and supervisors, at all levels, are responsible for the following:

- ensuring that all staff under their supervision, read and comply with this policy
- the safe, legal, ethical and responsible use of AI technology within their section, Branch or Division
- reporting any breach of this policy.

Managers must allow PM&C IT Security staff and internal Audit staff access to the AI technology that their team is authorised to use, to ensure compliance with their obligations.

## 4.7 AI business owners

Each AI technology, product and service that has been requested, assessed and authorised to be used within, and by PM&C, are to have a Business Owner. The Business Owner is responsible to the COO, that the AI technology, product or service is being used in accordance with this policy.

## 4.8 AI technical owners

Each AI technology, product and service that has been requested, assessed and authorised to be used within, and by PM&C, are to have a Technical Owner. The Technical Owner is responsible for the AI technology being used in accordance with this policy and is responsible for deployments and updating.

## 4.9 Authorised user responsibilities – AI

All users **must report** any AI related security incidents in accordance with the processes described in this policy.

Authorised PM&C users, regardless of position, accessing PM&C ICT resources to access approved AI products and services **must undertake the following**:

- read and acknowledge (through digital signature) this policy
- understand and comply with the [Australia's AI Ethical Principles](#) of use
- understand and comply with the [AI security rules](#) for development using AI technology
- obtain or have obtained written consent from ITSA on approval to access a specific AI technology
- ensure that only data / information that has been authorised to be used / uploaded into the approved AI technology, is used with that AI technology
- use available mechanisms and procedures to protect own information and information under their control
- notify appropriate managers of any perceived misuse of AI technology or any suspected violation of this policy
- not attempt to remove or circumvent security controls to access unauthorised AI technology on PM&C ICT assets
- report any suspected or suspicious access to ICT facilities using shared credentials, or credentials not belonging to an individual to the PM&C IT Security team.

## 5 AI account management

AI technologies, products, or services, offer different account plans, ranging from a basic (free) account to an enterprise-wide account. Some AI technologies offer subscription on a 'token' basis.

The level of functionality and capabilities offered by AI is dependent on the type / level of account purchased.

### 5.1 AI user account management principles / procurement

The following is to apply with regards to AI user accounts:

- no PM&C or shared services APS employee, consultant or contractor are to use their official credentials to create individual accounts on any AI platform, without having received approval from the Approving Authority
- the subscription purchase / procurement will be carried out by ICT Procurement
- the purchase may incur a cost to the acquiring business area
- Branches and Divisions **must not** purchase AI technology accounts without the written permission from the Approving Authority.

## 5.2 Responsibilities – business owner

The Business Owner for the AI technology/ platform is responsible for:

- the management of account access to their AI technology/platform
- ensuring that only their team members / staff have approval to access the approved AI technology.

Should other Branches / Divisions wish to access that AI technology or platform, they are to contact the Business Owner for that AI technology / platform and seek approval to use that AI platform. ITSA/CSO can request a risk assessment if required.

## 5.3 Responsibilities – ICT Procurement

ICT Procurement is responsible for:

- purchases of paid subscriptions and enterprise-wide AI technologies
- maintaining a register of AI technology subscriptions purchased for and on behalf of PM&C
- ensure any new product has been provided for review and investigation in accordance with relevant ICT policies prior to its procurement finalisation (i.e. contract execution or purchase).

## 5.4 User identification on AI platforms

All authorised users of any network **must** have a login ID which uniquely identifies the individual. Login IDs are not classified but should not be shared to external parties without consulting with the Cyber Security Team.

## 5.5 Multi-Factor authentication – AI products / services on approval of AI

s 47E(d)

s 47E(d)

## 5.6 Passwords

s 47E(d)

The following statements refer to the password use for any PM&C-managed systems, as well as any login credentials for online services used to process and store official information:

- passwords for the AI user account **must not** be divulged by the authorised users to non-authorised users
- if a password has been compromised or suspected to be compromised, it **must** be changed immediately, and the incident **must be immediately** reported to the PM&C IT Security Team
- s 47E(d)

# 6 Personal use of AI technology on departmental assets

## 6.1 Incidental personal use of AI on departmental assets

PM&C and other shared service agencies using PM&C systems recognise that users will want to test, learn, and use AI technologies, such as Microsoft Co-Pilot, to explore and understand the capabilities of AI. In seeking to maintain a balance between the needs of a user's agency and a user's personal requirements, and regarding the proper use of public funds, the use of PM&C ICT facilities incidental personal use is permitted provided that:

- it does not constitute an ongoing acceptable use in accordance with PM&C's policies
- its impact on the costs and operations on PM&C and/or any relevant shared service agency is negligible.

Under no circumstances, is any Australian Government information to be uploaded to an AI platform for personal use.

## 6.2 Monitoring of personal use

Users are to be aware that their use of PM&C's IT services and programs is monitored and logged for operational reasons to determine whether the networks are operating efficiently, to protect the security of the system and to isolate and resolve problems.

The department actively monitors staff use of the internet to identify unacceptable use and to determine compliance with this policy.

## 7 AI security incident reporting

The detection and reporting of AI related security incidents, breaches and violations are considered a contributor to ensuring the overall security of PM&C and must be reported as soon as the incident or suspected incident has been identified.

### 7.1 Reporting of an AI Technology - incident, breach, infringement, and/or violation

AI technology security incidents are a subset of the reportable security incidents for an agency. A reportable incident is any failure, suspected failure or identified deficiency which may result in a security exposure of an agencies ICT systems, or a compromise of PM&C or Australian Government information including personal information holdings.

Users **must** report AI technology security incidents, breaches, infringements and violations immediately / as soon as possible after detection or suspicion of activity.

Incidents are to be reported **immediately** to the PM&C IT Security Team – Email: [S47E@pmc.gov.au](mailto:S47E@pmc.gov.au)

If personal information is, or suspected to be involved, please copy the Privacy Team – Email: [privacy@pmc.gov.au](mailto:privacy@pmc.gov.au)

### 7.2 Appendix A – Australia's 8 AI ethics principles

[Australia's AI Ethics Principles](#) are designed to ensure AI is safe, secure and reliable. The following is the list of the Australia's 8 AI Ethics Principles:

1. **Human, societal and environmental wellbeing:** AI systems should benefit individuals, society and the environment.
2. **Human-centred values:** AI systems should respect human rights, diversity, and the autonomy of individuals.

3. **Fairness:** AI systems should be inclusive and accessible and should not involve or result in unfair discrimination against individuals, communities or groups.
4. **Privacy protection and security:** AI systems should respect and uphold privacy rights and data protection and ensure the security of data.
5. **Reliability and safety:** AI systems should reliably operate in accordance with their intended purpose
6. **Transparency and explainability:** There should be transparency and responsible disclosure so people can understand when they are being significantly impacted by AI, and can find out when an AI system is engaging with them
7. **Contestability:** When an AI system significantly impacts a person, community, group or environment, there should be a timely process to allow people to challenge the use or outcomes of the AI system.
8. **Accountability:** People responsible for the distinct phases of the AI system lifecycle should be identifiable and accountable for the outcomes of the AI systems, and human oversight of AI systems should be enabled.