Guidance for the use of artificial intelligence in Tasmanian Government

September 2024

PURPOSE OF THIS DOCUMENT

- To provide guidance for agencies to ensure a consistent baseline approach to the use of artificial intelligence by the Tasmanian Government.
- This document recognises the work being undertaken at a national level to provide a nationally consistent approach to the safe and ethical use of artificial intelligence by governments.
- Users of this guidance are advised that developments in AI are evolving quickly, and that guidance may depreciate with newly identified opportunities and risks, and technical developments.
- Release of this guidance was approved by the Tasmanian Government Secretaries Board 13 September 2024 and will be updated periodically, to reflect new developments.

SUMMARY OF KEY POINTS

- Innovation in artificial intelligence (AI) technologies has become major driver for opportunity and risk for Government.
- All jurisdictions in Australia have progressed policy or guidance linked to responsible and ethical use of AI.
- The guidance provided in this document is aligned with the national work that has been undertaken to develop the *National framework for the assurance of artificial intelligence in government*↗.
- This document outlines seven recommendations for agencies in relation to AI deployments:
    1. To deploy AI responsibly and ensure that that AI is deployed in a way that is safe, trustworthy, and ethical.
    2. Adopt a risk-based approach for specific uses and applications of AI.

3. Develop agency specific policy or guidance that is aligned with government and industry standards and frameworks.
4. Adopt consistent whole-of-government vocabulary for AI.
5. Build awareness and capabilities to develop, deploy and operate AI systems.
6. Align procurement practices with responsible deployment and risk assurance processes for AI.
7. Commit to whole-of-government cooperation and collaboration.

- Additional guidance is also provided with regards to the relevant policy, principles, considerations, and recommendations for various aspects of AI deployment, such as human, societal, and environmental impact, legal advice, transparency mechanisms, privacy, security, information, and data governance.

BACKGROUND

What is Artificial Intelligence?

- Artificial Intelligence (AI) is a domain of computer science that focuses on building computer systems to imitate human behaviour with a focus on developing models that can learn and can autonomously take actions on behalf of a human[1].
- AS/ISO 22989 defines an AI system as "an engineered system that generates predictive outputs such as content, forecasts, recommendations, or decisions for a given set of human-defined objectives."[2]
- AI systems encompass a variety of interrelated techniques and technologies, a basic overview is provided in table 1 (below).

Table 1 – Interrelated AI techniques and technologies

Generative AI	AI applications that when given some prompt or input can generate new content such text, images, audio, video, etc. When Generative AI solutions are combined with sophisticated language models that can interpret and replicate human language, an extremely effective method of communication between humans and machines/computers can be created.

[1] Info-Tech Research Group – provides technology research and advisory services for DPAC DSS.
[2] AS ISO/IEC 22989:2023 Information technology - Artificial intelligence - Artificial intelligence concepts and terminology

Machine Learning	A subset of AI that trains machines to learn from existing data and improve upon that data to make decisions or predictions. Deep learning is a more specialised machine learning technique in which more complex layers of data and neural networks are used to process data and make decisions[3].
Natural Language Processing (NLP)	A field of AI that deals with the ability of computer systems to understand and generate human language. NLP algorithms are used to analyse text, comprehend, converse with users, and perform tasks like language translation, sentiment analysis, and question answering[4].
Computer Vision	Systems that enable computers to 'see' and comprehend the visual world, analysing images and videos like humans. Computer vision algorithms analyse images and videos for tasks like object detection, face recognition, and self-driving cars[4].

The emergence and importance of Generative AI

- The recent emergence of Generative AI technology has extended the effectiveness, accessibility, and ease of use of AI technology enabling its integration into mainstream human activity, providing significant opportunity for innovation and productivity.

- Generative AI has the potential to assist workers by “automating well-defined and highly repetitive tasks, allowing them to then spend more time on the more complex aspects of their jobs. Generative AI can also augment and assist workers to complete more complex tasks, such as suggesting step-by-step problem-solving instructions or guiding workers through new skills and new ways of approaching problems”[5].

The opportunities of AI

- The value proposition of AI powered automation and advanced decision support are already well accepted across industry and government. AI solutions have been routinely deployed in a wide variety of applications and use within organisations for many years.

- The continued technological development and use of AI is expected to impact all sectors of the economy, improving existing industries and creating new products and services, and the use and development of modern AI technologies has significant ongoing potential to transform society and the economy.

[3] NZ Government, Interim Generative AI guidance for the public service, https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/interim-generative-ai-guidance-for-the-public-service/
[4] NSW Government, A common understanding: simplified AI definitions from leading standards, https://www.digital.nsw.gov.au/policy/artificial-intelligence/a-common-understanding-simplified-ai-definitions-from-leading
[5] Tech Council of Australia. “Australia’s Generative AI opportunity” (July 2023).

- For Government, the use of AI is likely to offer many benefits in efficiency and productivity enhancement through process simplification and automation, improved service design and methods of delivery, improved policy development through the classification and collation of large volumes of unstructured information.

Understanding the limitations and risk associated with AI.

- The use and deployment of AI is not without risk. Risks include the potential for bias, inaccuracy, lack of transparency and accountability. These issues are particularly important when working in the public sector. There are also issues relating to privacy and data protection, potential legal risks such as infringement of copyright and intellectual property, and in the worst cases the generation of malicious, fake, or illegal content[6].

- For many organisations the most likely diffusion of AI will be via the introduction and integration of AI into vendors' solutions and service offerings. This type of technology diffusion will be difficult to control, and some vendors may be protective of the intellectual property associated with their algorithms and capabilities.

- The Human Technology Institute (HTI) at the University of Technology Sydney recently published a comprehensive report that provides an excellent overview of risks/harms and some of the duty of care issues faced by organisations[7].

- The HTI report emphasises that beyond the generic commercial, regulatory, and reputational risks for organisations, AI systems have capacity to "cause real harm to people, both to individuals and society more broadly", including "threats to safety, discrimination, loss of personal information, and manipulation" along with the capacity "to amplify inequality, undermine democracy, contribute to unemployment, threaten security and increase social isolation".

- The HTI report also suggests that AI-related risks and harms flow from three sources – AI system failures, the malicious or misleading use of AI systems, and the overuse or reckless use of AI systems.

- There is now a greater awareness of AI in many sections of community and people are becoming increasingly concerned about AI-related risks. Only a third of Australians say that they trust AI systems, and less than half believe the benefits of AI outweigh the risks[7].

- With AI solutions becoming more and more pervasive and accessible, communities, industry and governments around the world are demanding that AI applications adhere to human-based values and take into consideration possible ethical and social impacts of the technology on society[8].

[6] DTA, Interim guidance on government use of public generative AI tools - November 2023
[7] Solomon, Lauren, and Nicholas Davis. "The state of AI governance in Australia." (2023).
[8] Info-tech Research, Build Your Generative AI Roadmap.

- The new challenge for industry and government is to ensure that AI is developed and used responsibly in a way that the community can trust that the technology is being used safely and appropriately in line with an underlying set of principles that reduces the risk of any unintended consequences.

Development of national principles for the ethical and responsible use of AI

- The Australian Government through the Department of Industry, Science and Resources maintains a *set of internationally aligned principles for AI Ethics*↗. This voluntary set of eight principles aims to – achieve safer, more reliable, and fairer outcome for all Australians, reduce the risk of negative impact on those affected by AI applications, and help businesses and governments to practice the highest ethical standards when designing, developing, and implementing AI [9].

- All government jurisdictions in Australia have progressed policy or guidance linked to responsible and ethical use of AI. Many jurisdictions actively engaged in significant AI capability development. Various industry groups and professional bodies have also developed principles, practices, and guidelines to address specific risks within their sector that are also applicable to government e.g., health, education, public safety, etc.

- In 2023 the Australian Government established the Artificial Intelligence (AI) in Government Taskforce that was focused on the safe and responsible use of AI by the Australian Public Service.

- Late in 2023 State and Territory Governments were invited to form a working group (through the Data and Digital Ministers forum) to codesign a nationally consistent approach for the safe and ethical use of artificial intelligence in Australia.

- The objective for this nationally consistent approach was ensure that AI projects are subject to a similar standard of risk assessment across jurisdictions, and to reduce any duplication of resources that may be spent developing individual processes and initiatives in isolation.

- On 21 June 2024, the Data and Digital Ministers endorsed the *National framework for the assurance of artificial intelligence in government*↗. This framework aligns with *Australia's AI Ethics Principles*↗and includes additional guidance common assurance practices.[10]

- Jurisdictions have agreed to align with the national framework as closely as practicable, understanding its application may differ according to jurisdictional specific governance and assurance protocols.

[9] https://www.industry.gov.au/publications/australias-artificial-intelligence-ethics-framework/australias-ai-ethics-principles
[10] https://www.finance.gov.au/publications/data-and-digital-ministers-meeting-outcomes/23-february-2024

AGENCY GUIDANCE

- The following recommendations are provided for Agencies to develop policy and guidance in relation to deployment and use of AI.

Recommendation 1. Deploy AI responsibly: ensure that that AI is deployed in a way that is safe, trustworthy, and ethical.

- Responsible deployment of AI means that those responsible and accountable for the design, development, and use of AI evaluate the impact of AI systems for both the Tasmanian Government and on the broader community and ensure that its use aligns with the *Australia's AI Ethics Principles*↗ (see also Appendix A).

- These Principles provide a set of internationally aligned directions for the ethical use of AI that can help guide the design, development, and use of AI within government.

- Responsible AI deployment includes the consideration of fairness and inclusivity, reliability and safety, the ability to interpret and explain system behaviour (transparency), protecting privacy and assuring the security of information assets.

- AI should be viewed as a complementary tool and the application and deployment of AI should ensure that "humans are retained in the loop', and that AI should not to be used in place of critical thinking.

- When AI is deployed responsibly, it can improve the efficiency, effectiveness, and quality of government services.

- Many industry and government sectors also provide similarly aligned principles that may be contextualised for those sectors.

Recommendation 2. Adopt a risk-based approach for specific uses and applications of AI.

- A risk-based approach should be adopted to assess the risk of the impact of AI technology in the context of specific uses and applications for the given appetite for risk set by an agency or by the Government as a whole.

- Risk assessments help to establish the controls needed to ensure the responsible deployment of AI (Responsible AI).

- This recommendation is consistent with the mandatory requirements set out in the *Protective Security Policy Framework (PSPF)*↗[11].

[11] Tasmania's Protective Security Policy Framework, https://www.dpac.tas.gov.au/__data/assets/pdf_file/0019/305335/Tasmanias-Protective-Security-Policy-Framework-TAS-PSPF.pdf

- It is important that Agencies take a balanced view of the opportunities and risk associated with AI. Like many technology solutions there are both low and high-risk scenarios associated with AI deployment. Many deployments will present significant opportunities for productivity and innovation and will not be high risk.

- In collaboration with State and Territories, the Australian Government released the *National framework for the assurance of artificial intelligence in government*↗ based on work undertaken by the NSW Government to develop guidance on AI risk assurance. The national framework emphasises taking a risk-based approach to AI in the adoption and deployment of AI solutions.

- AS/ISO 31000 Risk Management provides appropriate guidance for managing risk and undertaking risk assessment.

- The *NSW Artificial Intelligence Assurance Framework*↗ provides appropriate risk assessment guidance aimed specifically at AI projects and solutions.

Recommendation 3. Develop agency specific policy and guidance that is aligned with government and industry standards and frameworks.

- It is recommended that agencies develop policies and guidance aligned with their specific business requirements and the associated risks.

- Where policies and guidance are developed, it is recommended that Agencies consider how they align with *Australia's AI Ethics Principles*↗ and the *National framework for the assurance of artificial intelligence in government*↗.

- Additional considerations for aligning with the National AI assurance practices is also provided in the next section– *Additional considerations for aligning with national AI assurance practices.*

- Many industry sectors and areas of government have also developed standards and guidance for AI, where appropriate they should also be taken into consideration.

- National and international standards are also being established to address key aspects of AI; the following standards are particularly relevant –

    - ISO 22989 Artificial intelligence concepts and terminology – establishes terminology for AI and describes concepts in the field of AI.

    - ISO 38507 Governance implications of the use of artificial intelligence by organisations – provides governance guidance relating to the use of AI, in order to ensure its effective, efficient, and acceptable use within organisations.

    - ISO 42001 Artificial intelligence management system – specifies requirements for establishing, implementing, maintaining, and continually improving an Artificial Intelligence Management System within organisations.

Recommendation 4. Adopt consistent whole-of-government vocabulary for AI.

- The diffusion of AI technology has established new vocabularies to describe key concepts for emerging technologies and services. This vocabulary is often inconsistently applied or difficult to explain to people in non-technical terms. Notably there is not even a consistent definition for AI itself.

- To ensure we don't have divergent definitions for key concepts and to avoid misinterpretations, it is recommended that agencies adopt and contribute to the Tasmanian Government AI Glossary (See Appendix B).

- Acknowledging that there is likely to be sector specific terminology that would not be relevant for the Glossary.

Recommendation 5. Build awareness and capabilities to develop, deploy and operate AI systems.

- Agencies should ensure that employees have appropriate training, skills, and knowledge to develop, deploy and operate AI systems. This includes understanding the principles and requirements for responsible deployment of AI, and insight with respect to the capabilities, limitations and risks associated with the AI systems.[12]

Recommendation 6. Align procurement practices with responsible deployment and risk assurance processes for AI.

- It is important to have visibility and control over how vendors and service providers use or integrate AI into the solutions or services they provide.

- Whilst Agencies may plan to directly procure AI technologies, solutions, and services, it is more likely that vendors and service providers will introduce AI technology into their solutions or service offerings.

- Procurement teams should seek to evaluate the responsible AI and risk assurance guidance provided in *Australia's AI Ethics Principles*↗ and the *National framework for the assurance of artificial intelligence in government*↗.

- Where feasible key responsible AI and risk assurance concerns should be integrated into requirements documentation. Procurement teams may also consider including specific commercial protections in contracts.

[12] Adapted from the ANZPAA AI Principles for Policing jurisdictions.

Recommendation 7. Commit to whole-of-government cooperation and collaboration.

- It is recommended that agencies commit to a culture of collaboration and knowledge sharing across-agencies and for whole of government collaboration relating to AI.
- This includes –
    - participation in the codesign of policy, standards, and guidance.
    - supporting the alignment of approaches for the assurance of government use of AI.
    - establishing pathways to share knowledge such as AI solution patterns, collaboration on joint projects or sharing examples of newly identified risks, effective mitigation measures, and lessons learnt.
    - responding to newly identified opportunities and risks, technical developments, legislative change, and national and international developments.
    - Supporting the maintenance of a whole-of-government AI initiative register.

ADDITIONAL CONSIDERATIONS FOR ALIGNING WITH NATIONAL AI ASSURANCE PRACTICES.

- The following guidance is provided in relation to aligning with the assurance practices documented as part of the *National framework for the assurance of artificial intelligence in government*↗.
- The Tasmanian Government does not have a formal AI assurance framework of its own but has agreed to align with the *National framework for the assurance of artificial intelligence in government*↗ where practicable.
- Eight assurance practices are outlined in the *National framework for the assurance of artificial intelligence in government*↗ derived from work undertaken by the NSW Government as part of the *NSW Artificial Intelligence Assurance Framework*↗.
- The *NSW Artificial Intelligence Assurance Framework* is also a publicly available framework that provides more detailed guidance on the processes for undertaking a risk assessment of AI projects and initiatives against most of the assurance practices.

When should AI assurance processes be used?

- The assurance practices outlined in the *National framework for the assurance of artificial intelligence in government*↗ can assist agencies to design, build and use AI-enabled products and solutions by helping agencies to identify risks that may be associated with AI projects and initiatives.

- It is highly recommended that the assurance practices be considered in conjunction with the *NSW Artificial Intelligence Assurance Framework*↗ for initiatives that involve the design, development, deployment, and use of AI solutions that are high risk or include the use of large language models and generative AI.

- In instances of low risk, the evaluation of initiatives or solutions against the assurance processes may not be warranted. For example, you may not need to assess initiatives "that are using AI systems and data driven tools that are a widely available commercial applications (which you are not training, prompting or customising), and you are not using in any way that is a potentially elevated risk use case"[13].

- Agencies may also consider exempting or whitelisting specific solutions from requiring assessment where it is implicit that responsible AI requirements can be met, and any associated risk levels can be easily assessed as low.

CONSIDERATIONS

- Establish risk tolerances for use of AI assurance practices and processes that are aligned to your agencies risk management policy.

- In the absence of clear risk assessment guidelines, review the *NSW Artificial Intelligence Assurance Framework*↗ criteria for applying assurance processes and assess whether these criteria would be relevant to your agencies risk appetite.

- Assess projects and initiatives against the initial national framework's assurance processes and the guidance provided in this document, where risk tolerances are exceeded.

- Agencies should seek advice from the Tasmanian Government CIO or through the Tasmanian Government Data and Digital Subcommittee where they are uncertain on how to approach an AI assurance issue.

[13] NSW AI Assurance Framework https://www.digital.nsw.gov.au/policy/artificial-intelligence/nsw-artificial-intelligence-assurance-framework.

Legal advice

- Legal obligations in areas such as privacy, health information, discrimination, copyright, human rights and the role of AI in decision making are potential challenges for the deployment and use of AI solutions.

CONSIDERATIONS

- If AI is used for the purposes of automated decision making:
    - it should be supported by an appropriate legal foundation (including legislation);
    - humans must remain in the process; and
    - it cannot be used to replace the role of the human decision maker – for example, in a situation where penalties or sanctions may be imposed, the imposition of an appropriate penalty or sanction must not be automated, but instead be carried out by an appropriate human decision maker and then after her or him having turned her or his mind to the matter for determination and genuinely considered the matter on its merits.
- The inappropriate use of AI in decision making may expose the decision to the risk of legal challenge, including judicial review, including on the basis that it may be improper, unreasonable or has resulted in the denial of procedural fairness.
- Agencies should obtain legal advice from the Office of the Solicitor-General or the Office of the Crown Solicitor during the early stages of project development and at any stages during a project where they may have concerns or queries of a legal nature in relation to the use of AI (or otherwise more generally) including if at any stage if it is unclear whether use of AI:
    - complies with legal requirements, including in relation to its use or role in any decision-making process; or
    - otherwise presents legal risks.
- If copyrighted content is intended to be used to train an AI or even create work based on copyrighted content, its use requires the prior written permission of the copyright owner
- AI solutions may also require specific commercial protections in procurement contracts – for example what rights solution providers provide or have in relation to the use of specific data sets and models used in the solution, requirements to provide transparency mechanisms, or specific information security requirements or assurances.

Transparency mechanisms

- It should be made clear when AI tools are being used especially if AI was used to generate any of the information in briefings and official communications.
- When using AI tools, users need to be able to justify and explain their advice and decisions. They also need to critically examine outputs from these AI tools to ensure it reflects all relevant information and does not incorporate irrelevant or inaccurate information.

CONSIDERATIONS

- Users should ensure the ideas being generated by AI are ethical and responsible.
- Information provided by public AI tools is often not verified, may not be factual, or may be unacceptably biased. Users of AI tools should stop and think about where the data comes from and be aware of the nature of the tool being used.
- The United States Government National Institute of Standards and Technology (NIST) proposes *four principles for judging how well AI decisions can be explained*↗.
- Ensure there is an effective way to challenge an AI generated or informed decision.
- Consult with relevant community stakeholders when you design an AI system. This is particularly important for higher risk uses of AI.
- Create protocols or policy for attribution, tell people when you are using AI.

Privacy and data security

- The *National framework for the assurance of artificial intelligence in government*↗ provides significant guidance in relation to privacy and the protection of data. However, there are factors to be considered within the Tasmanian Government context.

CONSIDERATIONS

- Ensure that AI solutions and initiatives are compliant with the *Personal Information Protection Act 2004*↗.
- Ensure any inputs into ‘open’ or public AI tools (such as ChatGPT) will not include or reveal sensitive, classified, or personal information.
- Government information should only be entered into these tools if it has already been made public or would be acceptable to be made public. Ensure those determining that the information in question is suitable for public release have the appropriate organisational delegation to do so.

- Protected or sensitive information must not be entered into these tools under any circumstances. Similarly, Information that would allow 'open' or public AI platforms to extrapolate protected or sensitive information based on the aggregation of content entered over time should not be entered. This consideration also extends to contractors and consultants who are working with protected or sensitive information provided to them by government agencies.

- Undertake privacy impact assessments on initiatives that deploy or use AI. The Office of the Australian Information Commissioner (OAIC) provides authoritative *guidance and tools*↗ that can be adapted to assist with this process, noting that specific sectors such as Health and Education will have sector specific guidance.

- Develop a *privacy management plan*↗ for initiatives than involve the use of personal information.

Protective and cyber security

- The deployment and use of AI solutions need to ensure that protective security practices are followed.

- The Tasmanian Protective Security Policy Framework establishes the minimum protective security standards for Tasmanian Government agencies and their subsidiaries. This includes specific security requirements for information management and cyber security.

- The Tasmanian Government Cyber Security Policy outlines the principles, roles, and responsibility for managing cyber security risk across government. All agencies maintain cyber security policies, procedures, and guidance.

CONSIDERATIONS

- Where possible ensure that the information assets being used within an AI solution, model, or tool set are classified in accordance with the PSPF information classification requirements specified in INFOSEC-2 Core requirement 8.

- Undertake a cyber security threat and risk assessment (TRA) on AI tools and solutions and where that assessment identifies risk consider the development of appropriate cyber security controls.

- The Australian Signals Directorate (ASD) provides a comprehensive guide on how to use AI systems securely – *Engaging with Artificial Intelligence*↗.

- Protective security practices should also include consideration for – foreign ownership, control, or influence, mis/dis-information, and democratic integrity.

Information and data governance

- The decision rights and accountabilities for information and data related processes is essential for successful AI deployment.

- The Office of the State Archivist (OSA) maintains the *Tasmanian Government Information Management Framework*↗. The Framework identifies and defines the various components which contribute to effective information management.

CONSIDERATIONS

- Align standards and practices with *Tasmanian Government Information Management Framework*↗.

- Maintain or align with uniform standards and practices for data management. including data quality.

- The quality, accuracy, and fairness of AI systems heavily rely on the data used. Ensuring high-quality data inputs is essential for successful AI deployment.

- Ensure the data custodians are identified for data used in AI solutions and initiatives.

- When using AI solutions and tools considerations should be given to data residency and data sovereignty risks.

- Indigenous data sovereignty and governance – if you are you using Indigenous data, ensure the AI outputs are consistent with the expectations of First Nations peoples. The National Indigenous Australian Agency (NIAA) has released a *Framework for Governance of Indigenous Data*↗ which can be used as guidance.

RELEVANT LEGISLATION AND POLICY

- *Personal Information Protection Act 2004*↗ – governs the collection, use and disclosure of personal information. Schedule 1 of the act specifies the principles and requirements for the protection of personal information (privacy) by the Tasmanian Government.

- *State Service Code of Conduct*↗– reinforces and upholds the standards of behaviour and conduct that apply to all employees, including officers and Heads of Agency.

- *Tasmanian Anti-Discrimination Act 1998*↗ – makes discrimination and certain other conduct (such as sexual harassment) unlawful. It is discrimination when a person is treated less favourably (worse) than other people because they have a particular characteristic, such as their age, race, sex, or disability.

- *Tasmanian Government Cyber Security Policy*↗ – sets out the roles and responsibilities for agencies in relation to protecting Tasmanian Government information, systems, and services from cyber security threats.

- *Tasmanian Government Protective Security Policy Framework (PSPF)*↗ – establishes the minimum protective security standard required to provide protection, enabling resilience to compromise and harm. The PSPF addresses security outcomes required in the area of security governance, information security, personnel security, and physical security. The information security requirements of the PSPF are highly aligned with risk management issues associated with AI.

APPENDIX A – PRINCIPLES FOR THE ETHICAL AND RESPONSIBLE USE OF AI

Australia's AI Ethics Principles are proposed to be used for the national base approach. This will enable a flexible base for AI assurance that will allow national frameworks to develop over time in line with the quickly evolving nature of AI technology. Jurisdictions are encouraged to adapt these principles to their existing frameworks and ethics principles, as well as issuing additional guidance to support interpretation in their individual contexts.

Australia's AI Ethics principles are:

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 different 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.

APPENDIX B – TASMANIAN GOVERNMENT AI GLOSSARY

- Where appropriate the Tasmanian Government AI Glossary will align with ISO 22989 Artificial intelligence concepts and terminology, however preference will be to focus on providing plain English definitions and terminology in the first instance.

Glossary

- **Artificial intelligence (AI)** – is an engineered system that generates predictive outputs such as content, forecasts, recommendations, or decisions for a given set of human-defined objectives[2]. AI encapsulates a domain of computer science that focuses on building computer systems to imitate human behaviour with a focus on developing models that can learn and can autonomously take actions on behalf of a human[1].

- **AI assurance framework** – the processes and practices that ensure the safe, ethical, and effective development and deployment of artificial intelligence (AI) systems.

- **Computer vision** – Systems that enable computers to 'see' and comprehend the visual world, analysing images and videos like humans. Computer vision algorithms analyse images and videos for tasks like object detection, face recognition, and self-driving cars[4].

- **Cyber security** – the body of technologies, processes and practices designed to protect networks, computers, programs and information from attack, damage, or unauthorised access.

- **Cyber security threat and risk assessment (TRA)** – in the context of AI, a systematic process used to identify, assess, and remediate cyber risks associated with an AI system, solution or use case.

- **Data sovereignty** – ensuring that data remains within the jurisdictional boundaries and legal protections of its origin, impacting how it's stored, processed, and transferred.

- **Data governance** – the processes, policies, and standards put in place to ensure the availability, quality, and security of data.

- **Ethical impact** – behaviour impacting accepted standards of conduct or moral principles (notions of right and wrong). Applicable in both a social and professional context.

- **Generative AI (GenAI)** – AI applications that when given some prompt or input can generate new content such text, images, audio, video, etc. When Generative AI solutions are combined with sophisticated language models that can interpret and replicate human language, an extremely effective method of communication between humans and machines/computers can be created.

- **Large Language Models (LLMs)** – powerful computational machine learning models that excel at natural language processing tasks. LLMs are developed through the use of complex mathematical representations and statistical relationships of language associated with vast amounts of data.

- **Machine learning** – A subset of AI that trains machines to learn from existing data and improve upon that data to make decisions or predictions. Deep learning is a more specialised machine learning technique in which more complex layers of data and neural networks are used to process data and make decisions.

- **Natural language processing (NLP)** – A field of AI that deals with the ability of computer systems to understand and generate human language. NLP algorithms are used to analyse text, comprehend, converse with users, and perform tasks like language translation, sentiment analysis, and question answering.

- **Social impact** – impact on the wellbeing of communities and individuals.

APPENDIX C – SINGLE PAGE AI GUIDANCE REFERENCE