Artificial Intelligence Usage Policy

Technology and Innovation
Version: 1.0

Approved by: Deputy Minister, Technology and Innovation	**Owner:** ADM, Data and Content Management Division ADM, Cybersecurity Division	
Approval Date: May 1, 2025	**Last Reviewed:** May 2025	**Next Review:** May 2026
Contact: imt.policy@gov.ab.ca	**Policy Instrument type:** Policy	

Approval

This policy is approved by Janak Alford, Deputy Minister of Technology and Innovation.

Original signed by
Janak Alford, Deputy Minister of Technology and Innovation.
May 1, 2025

Date Approved
May 1, 2025

1. Purpose

1.1. The Government of Alberta (GoA) recognizes the transformative potential of artificial intelligence (AI) and will harness it to enhance service delivery for Albertans.

1.2. This policy enables and empowers GoA staff to use AI in a transparent, responsible, secure, ethical and human-centered manner.

1.3. This policy supports establishing Alberta as Canada's most AI-enabled public service.

2. Effective Date

2.1. The Artificial Intelligence Usage Policy takes effect on May 1, 2025.

3. Application

3.1. This policy applies to all departments defined under section 14 of Schedule 11 of the *Government Organization Act* and agencies, boards and commissions designated in Schedule 1 of the Freedom of Information and Protection of Privacy Regulation.

3.1.1. Agencies, boards, and commissions that are not designated in Schedule 1 of the Freedom of Information and Protection of Privacy Regulation are encouraged to align with this policy.

3.2. Contract managers will incorporate this policy where necessary when developing and/or managing relationships with third-party vendors, contractors, consultants, and/or any other organizations that provide services to (or perform services on behalf of) GoA departments.

3.3. This policy does not supersede any legislated obligations for privacy (e.g., Alberta and/or federal privacy legislation) and content management (e.g., the Records Management Regulation); legislation is paramount to this policy.

4. Definitions

4.1. **Artificial Intelligence System (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.
(Source: OECD AI Principles, April 2025)

5. Policy Statement

5.1. This policy enables GoA staff to use AI by establishing and promoting the responsibilities, obligations, and principles necessary to facilitate the responsible development, procurement, adoption, and/or implementation of AI by GoA departments.

5.2. AI use within the GoA is intended to benefit the public while maintaining public trust and safeguarding information in the custody and/or under the control of the GoA.

6. Policy Specifications

General

6.1. AI systems will be evaluated by Technology and Innovation (TI) through a coordinated approach (including, where necessary, security, privacy, content management, and/or legal review) to ensure that AI systems are trustworthy, subject to strong privacy controls (in alignment with the Privacy Management Framework), minimize data collection, operate as intended, and are secure against cyberattacks.

6.1.1. AI systems must be appropriate for the task (i.e., not more complex than necessary) and have built-in capacity for human intervention.

6.1.2. The GoA is committed to the development of a trust architecture in which multiple AI tools, human-centered processes, and effective governance build strong confidence in AI-enabled outcomes.

6.1.3. When necessary, the GoA will support sovereign compute capabilities to safeguard highly sensitive workloads for AI tools.

6.2. GoA staff may use approved AI systems (detailed in TI's listing of approved systems) in line with the usage recommendations and existing obligations (see below).

6.3. Business areas are accountable for all AI outputs (including, but not limited to, accuracy of outputs, alignment with privacy obligations, clearly labelling AI outputs, and ensuring alignment with applicable intellectual property obligations, etc.) and must be transparent regarding how AI outputs are used.

6.4. Unless specifically prohibited and/or rendered inaccessible (i.e., blocked) by TI, GoA staff may use unreviewed AI systems, provided that only publicly accessible content is used as inputs.

6.5. To expedite discoverability and promote innovation, business areas are encouraged to collaborate with TI to develop and/or leverage secure, controlled testing environments (i.e., "sandboxes") for exploring the feasibility of potential AI solutions; however, integration of AI solutions in GoA processes and/or service delivery is subject to TI review and approval.

GoA AI Principles

6.6. AI development, procurement, adoption, and/or implementation by the GoA must align with the following principles to ensure that AI use by the GoA is reliable, trustworthy, and benefits Albertans:

6.6.1. **Maintain security and privacy:** As AI systems may present potential (or unforeseen) risks, all staff must ensure they uphold their obligations to protect information (including personal information) in their custody and/or under their control from inappropriate or unauthorized access, use, disclosure, and/or destruction.

6.6.2. **Ensure strong ethics and mitigate bias:** As AI systems may generate harmful, biased, and/or unsafe outputs, AI development, procurement, adoption, and/or implementation by the GoA should seek to mitigate the effects of bias wherever possible to ensure fairness in outcomes and support public accountability. Ethics must be considered at every stage of development,

procurement, adoption and/or implementation, and staff must evaluate the ethical implications of AI on an on-going basis.

6.6.3. **Enhance trust:** To ensure public trust, the development, procurement, adoption, and implementation of AI by the GoA must be transparent, explainable, and clearly communicated. This includes alignment with notification requirements under applicable privacy legislation, and a clear explanation of what inputs are used and how outputs support human-centered service delivery.

6.6.4. **Maintain human control:** AI is a tool to support GoA operations and service delivery, not a replacement for human decision-making; AI will only be deployed and/or implemented where it is the best solution for a clear, well-defined issue. GoA staff will oversee AI systems and AI-supported processes, maintaining human accountability and ethical evaluation for AI outputs, service delivery outcomes, and any decisions enabled by AI-enabled solutions.

6.6.5. **Empower staff:** GoA staff are empowered to explore, develop, and improve AI-related skills (e.g., technical acumen, ethics) to ensure both currency and competency when leveraging AI.

6.7. AI systems may be regularly tested, audited, and/or evaluated by the relevant departments (i.e., TI) to assess their effectiveness, accuracy, suitability, and/or alignment to both existing obligations (e.g., applicable privacy legislation, content management requirements) and the principles established by this policy.

Existing Obligations

6.8. In addition to the legislated obligations to which all GoA staff must adhere (e.g., the Records Management Regulation, provincial privacy legislation), GoA AI development, procurement, adoption, and/or implementation must align with existing obligations, including (but not limited to):

- the Code of Conduct and Ethics for the Public Service of Alberta;
- the principles established by the Data Ethics Framework and the Privacy Management Framework; and
- the obligations and requirements established by IMT Policy Instruments for:
  - privacy (e.g., Privacy Breach Procedure);
  - content management (e.g., the Content Management Policy, Official and Transitory Records Directive);
  - security (e.g., the Cybersecurity Policy, the Information Security Management Directives, the Data and Information Security Classification Standard, etc.); and
  - technology operations (e.g., the Data Management Roles Directive).

AI Governance

6.9. The Deputy Minister of TI may identify new or existing governance bodies and/or roles, such as specialized working groups or collaboration teams, to support decision-making related to the development, procurement, adoption, and implementation of AI.

6.10. Departments will implement, and demonstrate compliance with, mandatory AI policy instruments.

- Exceptions may be available through a Statement of Acceptable Risk document (or a similar process/documentation) and will be administered on a

case-by-case basis at the discretion and approval of the Deputy Minister of TI in consultation with the appropriate Deputy Head(s).

7. Responsibilities

7.1. Deputy Heads will:

- maintain accountability for AI use in their respective departments;
- ensure AI use in their respective department aligns with relevant content and privacy management obligations, including collection notices (e.g., the Official and Transitory Records Directive, applicable privacy legislation);
- ensure that department-specific responsibilities for AI have been assigned, and are performed in alignment with applicable legislation and enterprise AI policy instruments;
- promote a culture of responsible AI use and appropriate risk management;
- support department staff participation in opportunities to build capacity, comfort, and familiarity with AI principles, systems, and operations; and
- undertake baseline productivity measurement (recommended) during adoption and/or evaluation of AI systems.

7.2. GoA staff (which includes, but is not limited to, employees, contractors, volunteers, appointees, and interns) will:

- adhere with content and privacy management obligations (e.g., the Official and Transitory Records Directive, applicable privacy legislation) to:
  - maintain official records regarding AI-related business decisions and transactions; and
  - protect information in their custody and/or under their control from inappropriate access, use, disclosure, and/or destruction.
- maintain current knowledge of, and adhere to, enterprise AI policy instruments developed by TI; and
- report potential AI issues or concerns through appropriate channels (e.g., Cybersecurity, an immediate supervisor).

7.3. Technology and Innovation will:

- establish government-wide (enterprise) direction for AI development, procurement, adoption, and/or implementation;
- champion all aspects of AI development in, and adoption by, the GoA;
- oversee development of data, security, privacy, and ethical performance metrics and accountability frameworks for AI development, procurement, adoption and/or implementation;
- monitor and evaluate data, security, privacy, and ethical practices to support beneficial AI-enabled outcomes;
- ensure GoA staff can build capacity, comfort, and familiarity with AI principles, systems, and operations;
- establish and maintain a list of approved AI platforms, systems, and use cases (including restrictions around unsafe workloads, and trial versions);
- guide departments on data, security, privacy, and ethical requirements when developing, procuring, adopting, and/or implementing AI systems; and
- report regularly to executive leadership on AI direction and outcomes, as necessary.

8. Compliance

8.1. Non-compliance with this directive could result in: the loss of content; breach of confidentiality; breach of privileged information; significant impact to GoA's proprietary rights; damage to GoA's reputation; exposure of Albertans to harm; and/or incurrence of unnecessary costs (including, but not limited to, inability to respond appropriately to a claim in court).

8.2. Depending on the severity of non-compliance:

- either informal or formal requests and/or follow-ups may be made by Innovation, Privacy and Policy Division, Corporate Internal Audit Services, Cybersecurity Services, Office of the Information and Privacy Commissioner, Office of the Auditor General and/or Public Service Commission; and
- legislated disciplinary action (i.e., *Public Service Act*) may be taken.

8.3. Non-compliance or violation of this directive must be brought to the immediate attention of the Cybersecurity Division and/or Privacy Services; these business areas will work with the appropriate department management to ensure that the problem is resolved, and necessary steps are taken to eliminate potential future violations.

9. References and Supporting Resources

9.1. The following resources are available to assist departments in adhering to this policy:

- Application Access Control
- Content Management Policy
- Data Ethics Framework
- Data Management Roles Directive
- Data and Information Security Classification Standard
- Information Controller and Information Custodian Directive
- Information Security Management Directive
- Official and Transitory Records Directive
- Privacy Management Framework

10. Contact

Types of Questions	Contact
Content Management	improgramsunit@gov.ab.ca
Cybersecurity	cybersecurity@gov.ab.ca
IMT Policy	imt.policy@gov.ab.ca
Privacy	privacy@gov.ab.ca

11. Review Date

11.1. This policy will be reviewed for accuracy and relevancy annually.

11.2. Interim updates to this policy may be made outside the established annual cycle if necessary (e.g., administrative updates related to government reorganization, emergency updates necessitated by significant legislative changes or technological advances, etc.).