



Hamilton Police Service Board Artificial Intelligence Systems Policy P-035

Effective date: July 23, 2026
Reviewed:
Amended:

Applicable Legislation

Subsections 37(1)(a) of the *Community Safety and Policing Act, 2019, S.O. 2019, c. 1, Sched. 1*, as amended (CSPA) provides that a Board shall provide adequate and effective policing in the area for which it has policing responsibility as required by Section 10 of the CSPA;

Subsection 38(1)(a) and 38(2) of the CSPA provides that the Board shall establish policies respecting the administration of the police service and may establish policies respecting any other matters related to the police service;

The Information and Privacy Commissioner of Ontario (IPC) and the Ontario Human Rights Commission (OHRC) have released joint Principles to guide the responsible adoption of Artificial Intelligence (AI) systems;

The Ontario Public Service (OPS) has issued a Directive on the Responsible Use of Artificial Intelligence (AI) that sets out the requirements for the transparent, responsible and accountable use of AI;

Definitions

For the purpose of this policy:

“Act” or “CSPA” means the *Community Safety and Policing Act, 2019, S.O. 2019, c. 1, Sched. 1*, and amendments thereto.

“Artificial Intelligence (AI) Systems” refers to any machine-based system or integrated set of technologies, data, processes, and human interactions that use computational methods, including machine learning, statistical modeling, or rule-based logic, to generate outputs such as predictions, recommendations, content, or decisions that influence operational, administrative, or public-facing outcomes. AI Systems include all components across their lifecycle, including data collection, model development, deployment, use, monitoring, and decommissioning, whether developed internally or procured from third parties. For greater clarity, AI systems may operate at varying levels of autonomy, but within Hamilton Police Service, they are to be used as decision-support tools and must not replace human judgment, professional discretion, or legal accountability. All AI-enabled outputs remain subject to human review, validation, and approval, in accordance with applicable laws, policies, and ethical standards.

“Bias” means incomplete, imbalanced or historically biased data, flawed algorithms, human use or unintended design choices, which may lead to systemic and unfair outcomes, such as discriminating against certain individuals or groups over another in ways that differ from the intended function of the algorithm, in the AI model outputs or decisions made.

“Board” means the Hamilton Police Service Board.

“Chief” means the Chief of the Hamilton Police Service.

“Human Rights AI Impact Assessment” means a tool that provides organizations with a method to assess AI systems for compliance with human rights obligations. The purpose of this human rights AI impact assessment (“HRIA” or “the tool”) is to assist developers and administrators of AI systems to identify, assess, minimize or avoid discrimination and uphold human rights obligations throughout the lifecycle of an AI system.

“Lifecycle” means the lifecycle of AI which includes the following stages: design, data and modelling; verification and validation; deployment; operation and monitoring; and decommissioning.

“Privacy Impact Assessment” means a process that reviews a new or existing information system or program to determine whether measures are necessary to ensure compliance with personal information protection requirements in statute and regulation and to address the broader privacy implications of the system or program.

“Service” means the Hamilton Police Service.

Policy Application

The Board deems it expedient to establish policies regarding the use of AI Technologies to ensure they are developed, acquired, used, and decommissioned in a manner that is responsible, transparent, and adhere to ethical standards, legal and regulatory requirements, and comply with relevant legal and regulatory frameworks, including, but not limited to, data privacy and security requirements.

The Board supports the responsible use of Artificial Intelligence (AI) Systems to enhance public safety, improve service delivery, and advance innovation. The Board is committed to ensuring the adoption and use of AI Systems align with the principles of fairness, transparency, accountability, and protection of privacy.

The Board will provide governance oversight of the Service deployment or enhancement of AI-enabled systems, particularly where such systems may present a moderate, high or critical risk of disproportionately impacting members of the community. In exercising this oversight, the Board will consider both the potential benefits of AI Systems and the need to safeguard the rights and well-being of individuals and communities.

The Board expects any use of AI Systems will comply with the applicable Canadian and Ontario laws and regulatory requirements, including those related to privacy, human rights, and individual rights and freedoms. The Service shall ensure the appropriate risk assessments, safeguards, and governance measures are in place, and decisions regarding the adoption and use of AI Systems are informed by evidence-based practices, including stakeholder engagement where appropriate, to identify and mitigate potential impacts.

Where appropriate, the Board may require reporting, evaluation, or review of AI-enabled systems to support transparency, accountability, and continuous monitoring throughout the lifecycle of such systems.

Section 1: Guiding Principles

The Board adopts the following IPC-OHRC Principles and ensures they are adhered to when considering the adoption and use of AI Systems. These principles are to be considered interconnected and of equal importance.

- **Valid and Reliable:** AI Systems must exhibit valid, reliable, and accurate outputs for the purpose(s) for which they are designed, used, or implemented.
- **Safe:** AI must be developed, acquired, adopted, and governed to prevent harm or unintended harmful outcomes that infringe upon human rights, including the right to privacy and non-discrimination.
- **Privacy Protective:** AI should be developed using a privacy by design approach. Developers, providers, or users of AI systems should take proactive measures to protect the privacy and security of personal information and support the right of access to information from the very outset.
- **Human Rights Affirming:** Human rights are inalienable, and protections must be built into the design of AI systems and procedures. AI systems must prevent and remedy discrimination effectively and ensure that benefits from the use of AI are universal and free from discrimination.
- **Transparency and Explainability:** The Service shall ensure that any AI Systems it develops, acquires, or deploys are implemented in a manner that is visible, understandable, traceable, and explainable supporting transparency, accountability and public trust.
- **Accountable:** The Service shall implement a robust internal governance structure with clearly defined roles, responsibilities, and oversight procedures, including a human-in-the-loop approach, to ensure accountability throughout the entire lifecycle of their AI Systems.

Section 2: Direction to Chief

2.1 Procedures

The Chief of Police shall establish the necessary procedures and processes defining the acceptable use and limitations on the deployment of AI Systems use by the Service.

2.2 Procedural Guidelines

The Chief of Police shall ensure the following guidelines are adhered to when considering the adoption and use of AI Technology and that the IPC-OHRC Principles are adhered to when considering the adoption and use of AI Systems:

- a. **Transparency:** In instances where the Service uses AI Systems which have an impact on decisions that affect members of the public, they must be given notice of such uses, unless full transparency may unduly impact the efficacy of investigative techniques or operations. In such cases, the Chief of Police will endeavour to make publicly available as much information about AI Systems as practicable, to assure the public of the reliability of the AI Systems and the justifiability of its use.
- b. **Accountability:** All use of AI Systems must be transparent and subject to performance measurement against recognized industry standards, supported by a clear governance framework, that ensures those responsible remain accountable for the decisions they make, including those informed or influenced by AI Systems or other algorithmic tools.
- c. **Fairness:** Use of AI Systems must not result in the increase or perpetuation of bias in policing and should seek to reduce the existence of such biases. The application of AI Systems in the delivery of police services must foster fairness by:
 - i. Ensuring equality and non-discrimination in AI operation;
 - ii. Protecting vulnerable groups from potential biases or adverse impacts
 - iii. Promoting diversity and accessibility in AI development and use; and

- iv. Enabling the review and correction of AI-supported decisions.
- d. Justifiability: The use of AI Systems must be shown to further the purpose of law enforcement in a manner that outweighs identified risks.
- e. Legality: All AI Systems used, and all use of AI Systems, in the course of delivering police services, must comply with applicable law, including the Community Safety and Policing Act (and its regulations, and successor legislation), Ontario's Human Rights Code, Municipal Freedom of Information and Protection of Privacy Act, the Information and Privacy Commissioner of Ontario, the Canadian Charter of Rights and Freedoms, and be compatible with applicable due process and accountability obligations.
- f. Public Engagement: Where appropriate and as contemplated below, public engagement can be crucial in establishing that AI Systems are used responsibly and takes a measured approach to the risk, cost, and community impact in the use of AI Systems.
- g. Privacy: Any use of AI Systems must protect personal and sensitive information that is collected, and must be proportionate and reasonable, and minimize potential risks and negative impacts.
- h. Reliability: AI Systems must demonstrate reliable and repeatable behaviour, producing AI outputs or recommendations that are consistent, while ensuring that any risks from inaccurate results are carefully assessed and avoided in contexts where factual accuracy or data integrity is essential.

2.3 Procurement and Approval

The Chief of Police shall:

- a. Ensure the appropriate industry standard risk assessment tools are incorporated into the review of AI Systems.
- b. Conduct a risk assessment of the AI Systems, prior to the earlier of:
 - i. Seeking funds for the new AI Systems, including but not limited to applying for a grant, or accepting municipal, provincial or federal funds, or public or private in-kind or other donations;
 - ii. Acquiring the new AI Systems, including acquiring such technology without the exchange of monies or other consideration;

- iii. Entering into agreements or where applicable, recommend the Board enter into agreements, to acquire, share, or otherwise use such AI Systems;
- iv. Not procure, utilize, or deploy a new AI Systems deemed to have a real risk of significant harm to the community, compromise the legitimacy of the Board or Service;
- v. When reporting to the Board and seeking approval for the procurement and deployment of AI Systems with a moderate, high or critical risk classification the report will describe, at a minimum:
 - 1. The operational need(s) the AI Systems will address, the intended use by the Service and how use of the AI Systems will improve on current practices or operations;
 - 2. Identify and where possible minimize the risk level assigned to the AI Systems, the rationale for the risk level assigned, and the rationale for continuing with the procurement, use or deployment despite the associated risk;
 - 3. The findings of a Privacy Impact Assessment and Human Rights AI Impact Assessment, and any risk analyses, including any analyses required by the Information and Privacy Commissioner of Ontario and the legislative authority for the collection of personal information;
 - 4. How the AI Systems operates, the source of the training data, and evidence of the validity, accuracy and security of the AI Systems under consideration, based on industry standards;
 - 5. An evaluation of the AI Systems vendor, including its record with regard to data security, privacy and ethical practices; and
 - 6. The estimated cost of acquiring and implementing the AI Systems.
- vi. Develop and implement a public engagement strategy for AI Systems with a moderate, high or critical risk classification, where appropriate, to transparently inform the public of the use of the AI Systems that collects data about members of the public or assists users in identifying, categorizing, prioritizing or otherwise making decisions pertaining to members of the public, prior to its deployment.

- vii. Once completed, the feedback received from consultations with relevant stakeholders and the general public will also be reported to the Board.

The Board shall:

- viii. Review the reports submitted and may determine;
 - 1. If additional analysis is required prior to approval of the procurement, deployment or use of the new AI Systems; and
 - 2. That the Service may initiate the procurement, deployment or use of the AI Systems, and identify any additional analysis, monitoring, auditing and reporting requirements beyond the ones required by this policy that are to be imposed once use of the AI Systems commences.

2.4. Deployment of AI Systems

The Chief of Police shall:

- a. Ensure the training of users of any AI Systems must address effective, legal, and ethical uses. Any follow-up training must be delivered to update the knowledge and skills of users as the AI Systems evolve.
- b. Consult with the stakeholders and impacted communities to identify and address any concerns arising from the use of AI Systems which are categorized with a moderate, high or critical classification. The results of consultations will be reported to the Board, including any actions taken to mitigate the risks and the harms of the AI Systems.
- c. Actively address and mitigate biases caused by the use of AI Systems to prevent discrimination against any community and ensure equitable outcomes.
- d. Prohibit the use of any existing AI Systems that poses a serious risk or is harmful to the community.

2.5. Data Privacy and Security

The Chief of Police shall:

- a. Implement and maintain privacy and confidentiality procedures which shall include strict protocols for the collection, storage, access, and sharing of data to be used by or for AI Systems, adhering to privacy laws and regulations.
- b. Ensure there are security measures to safeguard sensitive and personal information against unauthorized access and data breaches that will be caused by the improper use of AI Systems or any external cyber threats.

Reporting

To enhance accountability and transparency, the Chief of Police shall:

- a. Maintain and regularly update a public registry of AI Systems used by the Service. The registry must outline the capabilities, limitations, data handling practices, and purposes of the used technologies.
- b. Document the decision-making processes regarding the AI Systems including their selection, deployment, and use.
- c. On an annual basis, and as may be additionally required by the Board, provide a public written report to the Board that demonstrates compliance with this policy and an assessment of the achievements of the AI Systems according to the indicators established at the time the technologies were deployed. This report should include quantitative governance and performance indicators such as the AI Systems effectiveness; bias and fairness; compliance rates; data quality.

Background Information Relating to the Creation of the Board's Artificial Intelligence Systems Policy P-032

Governance Context: What the CSPA Requires

The CSPA reformed how police service boards govern their services. Two features of the Act are directly relevant to AI adoption:

- **Board oversight of "adequate and effective policing."** The CSPA shifts and clarifies the statutory responsibility for ensuring adequate and effective policing, and requires boards to set policies and hold the Chief accountable for how services are delivered. A board cannot discharge this oversight duty for a technology it has never reviewed, defined risk categories for, or required reporting on.
- **Compliance with the Human Rights Code and the Charter.** The Act's Declaration of Principles affirms that policing must be delivered in accordance with the Human Rights Code and the Canadian Charter of Rights and Freedoms. The Ontario Human Rights Commission has specifically flagged AI — including facial recognition and predictive policing tools — as a technology area where boards need Code-compliant procedures in place, since flawed training data or design can reproduce or amplify systemic bias against racialized and other marginalized communities.

Why the Policy Must Come Before, Not After, Use

a) Legal and liability exposure. Boards and services can face Human Rights Tribunal complaints, Charter challenges, or SIU/LECA scrutiny if an AI tool (e.g., facial recognition or predictive analytics) produces discriminatory outcomes. A pre-existing policy with documented risk assessment and mitigation steps is key to demonstrating due diligence.

b) Public trust and transparency. Communities need visibility into what tools are being used and why, before deployment, not through after-the-fact disclosure. A published inventory and risk framework, as TPSB adopted, is only credible if it precedes use.

c) Consistency with CSPA governance duties. Boards are required to set policy direction and hold Chiefs accountable. Approving AI use case-by-case without a governing policy undermines the board's statutory oversight role and creates inconsistent standards across units.

Ontario Public Service - Responsible Use of Artificial Intelligence Directive

This directive sets out the requirements for the transparent, responsible and accountable use of artificial intelligence (AI) by the Government of Ontario.

Updated: January 7, 2026

Published: January 7, 2022

1 Introduction

Artificial intelligence (AI) technologies provide considerable opportunities to advance innovation, improve service delivery, and save time and money for the people of Ontario. When used by the Government of Ontario, these technologies must be used in a way that protects the people, businesses and data of the province, preserves public trust, and in a manner that responsibly assesses and manages risk.

While risk is inherent to all technology, AI technologies are distinct in their potential to operate autonomously and make decisions. As a result, it can be difficult to determine how certain AI systems came to a given solution, which reduces transparency and could make it challenging to identify errors or dispute decisions. AI may also exacerbate existing biases and stereotypes^{[footnote 1\[1\]](#)}, potentially determining access to benefits or services in a discriminatory manner and infringing on human rights. These issues are compounded when individuals over rely on data or decisions produced by AI without sufficient human oversight, also known as technological deference or automation bias, which is the tendency to favour results generated by automated systems, even in the presence of contrary information from non-automated sources.

To ensure responsible, accountable and transparent use of AI in the Government of Ontario, ministries and provincial agencies must take a consistent, centralized approach to AI governance, have a common understanding of risks posed by AI, and consistently apply rules to manage these risks at every stage of the AI lifecycle, from the design to the development, procurement, deployment, operation and/or decommissioning of AI systems. Management of these risks would allow the Government of Ontario to realize the benefits and opportunities offered by AI while promoting a culture of shared responsibility over AI systems.

2 Purpose

The Responsible Use of Artificial Intelligence Directive (the “Directive”) sets out the requirements for the transparent, responsible and accountable use of AI.

3 Application and scope

The Directive applies to all Ontario ministries and provincial agencies. This Directive requires the application of AI risk management by ministries and provincial agencies that are seeking to use AI systems, or use services that include AI functionality (including procured, ministry/provincial agency developed and publicly available tools), as part of the development or delivery of, or decision-making for, a Government of Ontario policy, program, or service (referred to as a “use case”).

Infrastructure Technology Services or the appropriate Information and Information Technology (I&IT) Cluster, as the case may be, is accountable for applying AI risk management to enterprise Information Technology (IT) resources or systems that incorporate AI components and are consumed by ministries (or provincial agencies, as applicable).

Ministry and provincial agency executives are accountable for ensuring AI risk management of any IT resources and systems that may be built or used in the delivery of ministry-specific and provincial agency-specific programs and services, with the support of their I&IT Cluster, as appropriate.

Operational policies and guidance may provide additional support for the implementation of the Directive’s requirements, including how those requirements apply to AI use cases established prior to the Directive’s effective date.

4 Administration

The Directive is a Management Board of Cabinet Directive, issued under the *Management Board of Cabinet Act* and effective December 1, 2024.

The Secretary of Treasury Board (TB) and Management Board of Cabinet (MBC) has authority to issue operational policies that are consistent with this Directive.

The Ministry of Public and Business Service Delivery and Procurement (MPBSDP) is responsible for the Directive, and generally, will be responsible for any operational policies. Should any other program consider drafting an operational policy under this Directive, they must consult MPBSDP.

Ministries and provincial agencies must seek Management Board of Cabinet (MBC) approval if, in exceptional circumstances, they require an exemption from all or part of this Directive. Before seeking exemptions, program areas must consult MPBSDP as they prepare their request. The rationale for the exemption must be documented in a business case that requires MBC approval.

5 Responsible use of AI principles

The following 6 principles support the application of this Directive. The principles are meant to be applied in alignment with existing legislation, including the ethical framework established under the *Public Service of Ontario Act, 2006*, and help inform

decision-making when considering the use of AI systems (including procured, ministry and provincial agency developed and publicly available).

5.1 AI is used to benefit the people of Ontario

The people interacting with the AI system, and those affected by its outcomes, are considered when exploring potential AI use. The unique and diverse needs of users of government programs and services that leverage AI, and those affected by the outcomes of AI use, are accounted for in the design, operation and interpretation of outcomes. The tremendous benefits that can be realized by use of AI must be shared with the people of Ontario, while also ensuring that direct and indirect risks to the people of Ontario are mitigated and balanced with the benefits.

5.2 AI use is justified and proportionate, and AI systems used are reliable and valid

AI is only used where it serves a well-defined purpose, and the scope of AI use is proportionate to the problem it is trying to solve. Use follows a problem-first, rather than technology-first, approach. Once deployed, the AI system is reliable and valid – i.e., it works as intended and expected throughout its lifecycle.

5.3 AI is used in a safe, secure and privacy protective way

Data privacy and security are maintained in a way that protects personal and sensitive information and minimizes potential risks and negative impacts, as per Ontario privacy legislation and internal sensitivity policies. Any use or collection of personal or sensitive data is proportionate and reasonable, accounting for the potential benefit to the people of Ontario.

5.4 AI use is human rights affirming and non-discriminatory

AI is used in ways that respect and protect equity, human rights and fundamental freedoms and ensure fairness consistent with applicable legislation including the *Canadian Charter of Rights and Freedoms* and the *Ontario Human Rights Code*. Community-informed context, including an understanding of potential discriminatory outcomes and their mitigations, as well as inclusive design, are the foundations of determining if and how AI is used.

5.5 AI use is transparent and meaningful explanations of decisions are made available

Information is provided to the public and public servants about how AI is being used in a service or process, in a way that facilitates understanding of outcomes, consequences and benefits.

5.6 AI use is accountable and responsible

There is clear ongoing human oversight, accountability for, and maintenance of AI systems with a readily available process for the public and public servants to raise concerns about AI use.

6 Requirements

6.1 AI risk management

- ministries must engage in AI risk management when seeking to use AI systems for a Government of Ontario use case. AI risk management aligns with the Ontario Public Service (OPS) Risk Management Process
- to manage AI risk, ministries must:
 1. 1. State objectives and establish context.
 1. a. Document the problem AI use is intended to solve.
 2. b. Determine whether AI use is justified.
 2. 2. Identify risks.
 3. 3. Assess risks.
 1. a. Determine the risk level of the AI use to inform potential risk-based proportional controls.
 4. 4. Plan and take action.
 1. a. Identify and apply risk-based proportional controls.
 5. 5. Report and monitor.
 1. a. Monitor and update risk assessment to ensure proportional controls remain current and are re-applied as necessary.
- AI risk management must be validated by IT and digital governance processes and does not duplicate or replace existing processes (Privacy Impact Assessments, Threat Risk Assessments). Operational policy and guidance may specify further direction on AI risk management governance and approvals

6.2 Disclosure and reporting

- ministries must report on AI use cases and AI risk management, including identified risks related to AI use, to MPBSDP annually
- ministries must coordinate with MPBSDP to publish a list of AI use cases
- if the public is interacting directly with a service that leverages AI (for example, a chatbot) or if AI is involved in decision-making directly affecting a member of the public (for example, determining eligibility for a government service or benefit), then ministries must also:
 - publicly disclose AI use as part of the process, service, or program
 - provide an accessible avenue for the public to seek information about the use of AI in a process, service, or program. This does not create a new avenue for seeking review of decisions – existing legislative avenues to

appeal a decision or outcome of a process, service or program continue to apply

6.3 Application to Provincial Agencies

Provincial agencies must:

- where using AI as part of the development or delivery of, or decision-making for, an agency-specific policy, program, or service, in alignment with Section 3 (Application and Scope), implement AI risk management in alignment with the principles under section 5 and requirements under section 6.1, including establishing approvals processes for AI use based on risk level
 - keep records associated with AI risk management, including records of any risk assessments and risk-based proportional controls applied, in alignment with existing Records and Information Management and archiving requirements
- publish a list of AI use cases and report on AI use cases and AI risk management, including identified risks related to AI use, to their accountable ministry in alignment with requirements in the Agencies and Appointments Directive and Provincial Agencies Memorandum of Understanding, including any necessary supporting information and analysis
- if the public is interacting directly with a service that leverages AI (for example, a chatbot) or if AI is involved in decision-making directly affecting a member of the public (for example, determining eligibility for a government service or benefit), then:
 - publicly disclose AI use as part of the process, service, or program
 - provide an accessible avenue for the public to seek information about the use of AI in a process, service, or program. This does not create a new avenue for seeking review of decisions – existing legislative avenues to appeal a decision or outcome of a process, service or program continue to apply

7 Roles and responsibilities

The accountabilities detailed below attach to these entities or successor organizations who inherit these mandates (through organizational restructuring or name changes).

7.1 Treasury Board and Management Board of Cabinet

- approve this Directive and any changes to it
- approve exemptions from this Directive in whole or in part through review of a submitted business case
- receive annual report from MPBSDP about AI risk management, including a list of AI use cases across the Government of Ontario and identified risks related to AI use

7.2 Secretary, Management Board of Cabinet

- approve updates, exemptions and operational policies pursuant to this Directive
- recommend updates to this Directive to Treasury Board/Management Board of Cabinet

7.3 Deputy Ministers and Provincial Agency Heads or equivalent

- ensure the Directive's principles and requirements are implemented and monitored throughout their ministry and provincial agency, including putting in place processes that support the Directive
- ensure that provincial agencies for which Deputy Ministers are accountable are aware of the requirements of this Directive
- ensure that all persons covered by this Directive are aware of their responsibilities under this Directive
- in the case of provincial agencies, provincial agency heads or equivalent must also establish approvals processes for AI use based on risk level

7.4 Deputy Minister Committee on Service Delivery

- provide advice on strategic direction for AI adoption and risk management across the Government of Ontario
- issue communications and guidance based on emerging trends or issues in AI technology

7.5 Associate Deputy Minister, Policy, Archives, and Data (PAD)

- maintain this Directive and support its implementation
- develop and maintain strategic policy, as well as operational policies, standards, guidelines and best practices governing responsible use of AI and data pursuant to this Directive, as required
- conduct reviews of the Directive and supporting material, every two years at a minimum, and recommend any changes
- work with the Corporate Chief Information Officer to raise awareness of and promote compliance with AI and information security policies, standards and guidelines across the Government of Ontario
- ensure alignment between AI use and data privacy protection and freedom of information requirements and policies, including the *Freedom of Information and Protection of Privacy Act* and the *Personal Health Information Protection Act*
- support education, training and implementation of Directive requirements

7.6 Office of the Chief Risk Officer

- oversee the OPS Enterprise Risk Management process, including reviewing and advising on ministry risk information and risk management practices

- work in cooperation with ministries and central agencies to ensure that risk information is available to MPBSDP

7.7 Chief Information Security Officer

- provide advice and guidance to ministries, provincial agencies and other partners to ensure that security considerations are incorporated into AI planning, procurement, deployment, use and ongoing management.
- identify appropriate security controls for AI and ensure that they are implemented in accordance with security policy and standards, security testing, and assessment or evaluation recommendations (or that residual risks are documented and accepted).
- ensure cyber risk management policies, standards, requirements and processes are incorporated into AI use and evaluate for continuous compliance.
- work with policy and operational partners (for example, Associate Deputy Minister, PAD and Corporate Chief Information Officer) to provide advice and guidance, create and raise AI security awareness and training to the enterprise.
- take action to block or stop any activities posing imminent security risk of significant impact, implement necessary security protocols, conduct thorough investigations into potential breaches, and collaborate with relevant authorities as needed.

7.8 Corporate Chief Information Officer

- develop and maintain technology-focused and implementation operational policies, standards, guidelines and best practices pursuant to this Directive, as required
- provide advice and guidance to ministries and provincial agencies on potential opportunities to derive value from AI, while abiding by the principles of this Directive
- adhere to the requirements of the AI Directive when operationalizing enterprise technology programs and services, in collaboration with ministry executives and provincial agency heads
- consult with the Deputy Minister Committee on Service Delivery on issues related to AI use, related cyber security concerns and emerging AI trends
- submit reporting on AI use cases, AI risk management and risks related to AI to TBS annually
- receive and review additional risk information, including from the Office of the Chief Risk Officer, to support the monitoring and tracking of AI related risks
- work with the Associate Deputy Minister, PAD to raise awareness of and promote compliance with AI policies, guidelines and standards across the Government of Ontario

7.9 All ministry and provincial agency employees

Act in accordance with this Directive, as well as any other policies, guidance and standards that further define obligations relating to the responsible use of AI.

8 Definitions

For the purposes of this Directive, these terms have the following meaning:

Artificial intelligence (AI) system: An AI system is a machine-based system that, for explicit or implicit objectives, makes inferences, from the input it receives, in order to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. (Aligned with Organisation for Economic Co-operation and Development (OECD), 2024).

AI lifecycle: The AI lifecycle encompasses the following phases that are not necessarily sequential: planning and design; collecting and processing data; building and using the model; verifying and validating; deployment; and operating and monitoring (OECD, 2019).

AI use case: A purposeful application of an AI system to a project or initiative (whether it be policy, program or service) to achieve a specific outcome.

Biases: A predisposition, prejudice or generalization about a group of persons based on personal characteristics or stereotypes (Ontario Human Rights Commission Glossary of Human Rights Terms, 2013).

Community: In the context of this Directive, community specifically references affected groups, including traditionally marginalized groups and people who are systemically excluded from decision-making, public institutions, basic services and meaningful participation in economic, political and social activity.

Discrimination: Treating someone unfairly by either imposing a burden on them, or denying them a privilege, benefit or opportunity enjoyed by others, because of their race, disability, sex or other personal characteristics identified under the *Ontario Human Rights Code*. Systemic discrimination refers to where institutional behaviour, policies, practices and procedures create or perpetuate inequality for groups identified under the Ontario Human Rights Code (*Ontario Human Rights Commission, 2024*).

Risk: The effect of uncertainty on objectives. It can be characterized as either a potential negative (threat) or positive (opportunity) consequence or event that deviates from an expected outcome (*OPS Enterprise Risk Management Directive, 2020*).

Risk management: A systematic approach to setting the best course of action under uncertainty by identifying, assessing, understanding, acting on, monitoring, and communicating risk issues (*OPS Enterprise Risk Management Directive, 2020*).

Validity: Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled. Deployment of AI systems which are inaccurate, unreliable, or poorly generalized to data and settings beyond their training, creates and increases negative AI risks and reduces trustworthiness (National Institute of Standards and Technology, U.S. Department of Commerce, 2023).