ONTARIO · BILL 194 / ENHANCING DIGITAL SECURITY AND TRUST ACT

Bill 194 AI Readiness Checklist

A working readiness checklist for the AI transparency, accountability, risk-management and human-oversight expectations that apply to Ontario municipalities.

Municipality	[Insert municipality name]
Prepared by	[Insert name and title]
Date	[Insert date]
Status	Readiness tool — not legal advice

Contents

Why this checklist exists 3

1. Governance and accountability 3

2. Inventory and risk classification 4

3. Transparency and public information 4

4. Human oversight 5

5. Risk management 5

6. Data, privacy and security 6

7. Procurement and vendor management 6

8. Monitoring, incidents and review 7

9. How TrueNorth supports each area 7

10. Attestation 8

Why this checklist exists

Bill 194 Schedule 1 applies AI transparency, accountability, risk-management and human-oversight expectations to prescribed public sector entities, including MFIPPA institutions. The regulations are still being phased in, so the checklist is built to be useful now and adjustable later.

> **HOW TO USE IT**
> Work through the sections with the people who own each area. For every item, record an owner and the evidence that shows it is in place — a policy number, a council resolution, a meeting minute or a link to a public page. The point is to be able to show a coherent governance story, not to produce a perfect binder. Items marked “not applicable” should say why.

1. Governance and accountability

TABLE 1 · GOVERNANCE AND ACCOUNTABILITY

Readiness item	Status	Owner	Evidence
Council or CAO has adopted an AI-use policy covering approved tools, permitted uses and prohibited uses.	☐	[Insert]	[Insert]
A named responsible officer is accountable for AI use and for pausing or withdrawing a tool if needed.	☐	[Insert]	[Insert]
Roles and responsibilities are documented for staff, IT, the privacy lead and the CAO.	☐	[Insert]	[Insert]
An AI inventory exists and records each tool, its purpose, its risk level and its review date.	☐	[Insert]	[Insert]
A process exists for approving a new AI tool before use, including privacy, security and records review.	☐	[Insert]	[Insert]
Staff know how to report a concern, error or suspected misuse.	☐	[Insert]	[Insert]

2. Inventory and risk classification

TABLE 2 · INVENTORY AND RISK CLASSIFICATION

Readiness item	Status	Owner	Evidence
Each AI tool is classified by risk (for example, low / moderate / high) using a documented method.	☐	[Insert]	[Insert]
The classification considers whether the tool informs decisions about individuals.	☐	[Insert]	[Insert]
A model or system card exists for each tool, describing what it does and does not do.	☐	[Insert]	[Insert]
Tools that are no longer used are recorded as retired, with data disposition noted.	☐	[Insert]	[Insert]

3. Transparency and public information

TABLE 3 · TRANSPARENCY AND PUBLIC INFORMATION

Readiness item	Status	Owner	Evidence
A public page explains which AI tools the municipality uses and for what purposes.	☐	[Insert]	[Insert]
The page is written in plain language and is linked from the municipal website.	☐	[Insert]	[Insert]
The page explains how a resident can ask a question or raise a concern about AI use.	☐	[Insert]	[Insert]
The page is reviewed when a tool is added, changed or retired.	☐	[Insert]	[Insert]
Council receives a short periodic report on AI use, incidents and changes.	☐	[Insert]	[Insert]

4. Human oversight

TABLE 4 · HUMAN OVERSIGHT

Readiness item	Status	Owner	Evidence
All AI-assisted outputs are reviewed by a named staff member before use in a decision, communication or record.	☐	[Insert]	[Insert]
No AI tool makes an autonomous decision about an individual's rights, benefits, eligibility or enforcement.	☐	[Insert]	[Insert]
The reviewer has the authority and information needed to reject or correct an AI output.	☐	[Insert]	[Insert]
Staff training covers the limits of AI output, citation checking and the requirement to verify facts.	☐	[Insert]	[Insert]
Where a decision affects an individual, the municipality can explain how the tool was used and what human oversight applied.	☐	[Insert]	[Insert]

5. Risk management

TABLE 5 · RISK MANAGEMENT

Readiness item	Status	Owner	Evidence
A PIA has been completed for each AI tool that processes personal information.	☐	[Insert]	[Insert]
A documented risk assessment covers accuracy, bias, privacy, security and public trust.	☐	[Insert]	[Insert]
Mitigations are recorded with an owner and a review date.	☐	[Insert]	[Insert]
Residual risk is accepted by the appropriate authority and recorded.	☐	[Insert]	[Insert]
Risks are reassessed when the tool, its use or its vendor changes.	☐	[Insert]	[Insert]

6. Data, privacy and security

TABLE 6 · DATA, PRIVACY AND SECURITY

Readiness item	Status	Owner	Evidence
Personal information flows are mapped, including any processing outside Canada.	☐	[Insert]	[Insert]
Retention and deletion are configured and recorded in the PIA.	☐	[Insert]	[Insert]
Access is role-based and reviewed when staff change roles.	☐	[Insert]	[Insert]
The vendor contract includes confidentiality, data-processing, breach-notification and deletion commitments.	☐	[Insert]	[Insert]
A breach-response procedure addresses the RROSH threshold and IPC reporting, effective January 1, 2027.	☐	[Insert]	[Insert]

7. Procurement and vendor management

TABLE 7 · PROCUREMENT AND VENDOR MANAGEMENT

Readiness item	Status	Owner	Evidence
AI-specific terms are included in the contract or procurement documents.	☐	[Insert]	[Insert]
The vendor has disclosed its data residency, subprocessors and model-training practices in writing.	☐	[Insert]	[Insert]
The vendor has committed to notify the municipality of material changes to the service or its subprocessors.	☐	[Insert]	[Insert]
An exit plan exists: how records are exported and deleted if the municipality changes vendors.	☐	[Insert]	[Insert]
The purchase route is documented against the municipal purchasing bylaw.	☐	[Insert]	[Insert]

8. Monitoring, incidents and review

TABLE 8 · MONITORING, INCIDENTS AND REVIEW

Readiness item	Status	Owner	Evidence
AI use is reviewed at least annually, and after any significant incident.	☐	[Insert]	[Insert]
Incidents involving AI are logged and assessed through the municipality's privacy and security processes.	☐	[Insert]	[Insert]
Staff can pause use of a tool if it produces unsafe or unreliable output.	☐	[Insert]	[Insert]
Changes to the tool, its use or the vendor trigger a review of the PIA and this checklist.	☐	[Insert]	[Insert]

9. How TrueNorth supports each area

This table shows which items the platform supports directly, which are documentation the municipality owns, and which are policy choices only the municipality can make.

TABLE 9 · PLATFORM SUPPORT MAP

Readiness area	Platform support	What the municipality still owns
Governance and accountability	Governance Hub with document templates and assessment records on qualifying plans.	Adopting the policy, naming the responsible officer and recording council approval.
Inventory and classification	AI inventory and model registry with risk levels.	Deciding which tools are approved and reviewing the inventory.
Transparency	Public transparency pages and platform metrics.	Publishing the municipality's own plain-language page and contact channel.
Human oversight	Human-in-the-loop checkpoints in every workflow; cited sources.	Assigning reviewers and enforcing the "no autonomous decisions" rule.
Risk management	PIA and algorithmic impact assessment templates; compliance scanner.	Completing, signing and retaining the assessments.
Data and privacy	Canadian residency, DLP, encryption, retention and audit logs.	Configuring retention to the records schedule and completing the PIA.
Procurement	Security brief, data-processing terms, procurement documentation.	Following the municipal bylaw and approving the contract.
Monitoring and review	Audit logs and usage reporting.	Annual review, incident assessment and council reporting.

10. Attestation

This checklist is complete when the municipality can point to evidence for each item — not when every box is ticked.

Role	Name	Signature	Date
Responsible officer	[Name and title]		
Privacy lead	[Name and title]		
CAO or delegate	[Name and title]		

This checklist is a readiness tool. It is not legal advice, and it does not certify compliance with the Enhancing Digital Security and Trust Act, 2024 or its regulations. The Act's AI provisions are being phased in through regulations; requirements may change. Confirm current obligations with the Information and Privacy Commissioner of Ontario, the Ministry and your own legal advisor.