BRITISH COLUMBIA · FOIPPA S.69(5)

Privacy Impact Assessment

A pre-filled working template for a British Columbia public body assessing the TrueNorth Civic AI platform. Vendor facts are completed; public-body fields are marked for your review.

Public body	[Insert public body name]
Service assessed	TrueNorth Civic AI
Assessment date	[Insert date]
Status	Draft for review — not legal advice

Contents

How to use this template 3

1. Purpose and Scope 3

2. Public Body and Service Information 4

3. Personal Information Inventory 4

4. Personal Information Flow Map 5

5. FOIPPA s.69(5) Notice Requirements 6

6. Security and Privacy Safeguards 7

7. Retention and Disposal Schedule 8

8. Residual Risks and Mitigations 8

9. Approvals and Sign-Off 9

Appendix A: Attachments 9

How to use this template

This is a working document, not a marketing artifact. It is structured so a British Columbia public body can complete its own privacy review without outside counsel, while keeping every vendor fact verifiable.

1. Complete the bracketed fields. Anything shown as [Insert ...] is specific to your public body and must be completed by you. Vendor facts are already filled in.
2. Delete what does not apply. If a category of personal information is not in scope, say so explicitly rather than leaving the row blank. A short, accurate PIA is better than a long, vague one.
3. Review with the person who will sign it. For most local governments this is the Chief Administrative Officer, Clerk or designated privacy lead, in consultation with IT.
4. Record the approval decision. State whether the deployment is approved, approved with conditions, or not approved — and who made that decision.
5. Retain and update. Keep the signed PIA with the procurement file. Update it before any significant change in purpose, and provide a copy to the Office of the Information and Privacy Commissioner for British Columbia on request.

LEGAL STATUS

This template is provided for information and procurement support. It is not legal advice. Your public body remains responsible under FOIPPA for determining how the Act applies, for completing and approving this assessment, and for its own notice, retention and breach-response practices.

PRE-FILLED VENDOR FACTS

Sections marked “Vendor-completed” contain facts supplied by TrueNorth Civic AI about the platform’s architecture, safeguards and retention. Verify them against the companion IT Security and Architecture Brief and, where you wish, against the platform configuration during onboarding.

1. Purpose and Scope

This Privacy Impact Assessment (PIA) is prepared for use by British Columbia public bodies — municipalities, regional districts and other local government organizations — considering or deploying the TrueNorth Civic AI platform.

It is a pre-filled working template: the platform-side data flows, safeguards and retention facts are completed by the vendor, while public-body-specific fields are left as bracketed placeholders for review and completion by your Information Access and Privacy function. This document supports, but does not replace, your public body’s own PIA approval process, and should be adapted to your institution’s risk context and to any additional systems in scope.

SCOPE OF THIS ASSESSMENT

- In scope: the TrueNorth Civic AI web application, the AI processing pipeline, document storage, tenant administration and the vendor’s support arrangement, as configured for your public body.
- Out of scope: other municipal systems that may exchange records with the platform, and any use that is not described in Section 3.

2. Public Body and Service Information

Public body	[Insert public body name]
Public body type	[Municipality / regional district / other local government body]
Department or program	[Insert the department or program sponsoring use]
Service under assessment	TrueNorth Civic AI — a cloud AI workspace for municipal staff providing legislative and bylaw research (retrieval from BC statutes and municipal bylaws), document drafting, meeting transcription and minutes, workflow automation, and analytics.
Users in scope	[Insert number of users and roles — up to the seat capacity of the purchased plan]
Vendor	TrueNorth Civic AI · support@truenorthcivicai.ca · truenorthcivicai.ca
Assessment date	[Insert date]
Version and next review	[Insert version] / [Insert date or review trigger]

3. Personal Information Inventory

The categories below are expected to flow through, or be stored in, the platform. Confirm each category against your own records and delete any that do not apply.

1. Staff account data — name, work email address, department, job title and an optional profile photo. Used for account administration and display.
2. User-generated content — chat questions, drafts, uploaded records and meeting transcripts. These may contain third-party personal information (for example resident names, addresses and telephone numbers) when staff process municipal records. Used to perform the requested research, drafting or analysis for the public body.
3. Support and feedback data — support correspondence and feedback submissions, including the platform's public feedback channel, which transmits to the vendor's support channel.
4. Audit and telemetry data — timestamps, user identifiers and action logs used for governance reporting and incident investigation.
5. Special categories — [identify any health, law enforcement or other sensitive records in scope, or state "none"].

> **DATA MINIMISATION**
> Staff should enter only the personal information the municipal purpose requires. The platform redacts detectable Canadian identifiers before any model call, but redaction is a safety net, not a substitute for collecting and entering less.

4. Personal Information Flow Map

The table below maps each processing stage to its system, location and safeguards. Locations are stated as configured in production, not as a general corporate capability.

TABLE 1 · PERSONAL INFORMATION FLOW MAP

Stage	System / service	Location	Safeguards
Sign-up and identity	Firebase Authentication (work email, verified) with optional Microsoft Entra ID (Azure AD) single sign-on	Canada / global identity service	Government-organization email verification; optional Microsoft 365 work-account sign-in matched to the tenant by verified email domain; minimal profile data (name, work email, department, job title)
Transmission	HTTPS to the TrueNorth API and Firebase	In transit to GCP northamerica-northeast1	TLS 1.3 encrypted transport; HSTS
Pre-processing	Cloud DLP inspection and redaction before any model call	Google Cloud DLP global endpoint (processing not region-pinned); results stored in Montréal	Canadian identifiers (SIN, PHN, addresses, contact information) are detected and redacted before AI processing
AI processing	Vertex AI (Gemini models) with web grounding disabled by default on sensitive workflows	US/EU multi-regions (Gemini 3.x via the Vertex AI global endpoint; embeddings run in Montréal)	Zero model training on customer data; prompts and outputs are Customer Data and not retained by the model provider beyond transient processing; DLP pre-redaction runs before every model call
Document storage	Cloud Storage and PostgreSQL (documents, retrieval indexes)	northamerica-northeast1 (Montréal)	AES-256 at rest; customer-managed encryption keys (CMEK) on qualifying plans; tenant isolation
Retention and purge	Scheduled data-retention jobs	northamerica-northeast1 (Montréal)	Chat threads auto-purge after 30 days; uploaded documents are retained 90 days (configurable by agreement); deletion on request or at termination

Identity verification is performed by Firebase Authentication. Where your public body uses Microsoft 365, optional Entra ID single sign-on matches staff accounts to your tenant by verified email domain; no directory data beyond the sign-in profile is copied into the platform.

5. FOIPPA s.69(5) Notice Requirements

FOIPPA s.27 requires notice at or before collection. The checklist below maps the s.69(5) PIA notice elements to vendor facts that are already completed and to the fields your public body must complete.

TABLE 2 · FOIPPA S.69(5) NOTICE REQUIREMENTS

Requirement	Pre-filled TrueNorth side	Public body to complete
(a) The purposes for which the information is collected	Collection is limited to municipal staff using the platform: identity and account administration, internal research and drafting for municipal programs, and service-support communication	Adapt the purpose statement to your program name and department
(b) The specific legal authority for the collection	To be completed by the public body; commonly FOIPPA s.26(c) (necessary for an operating program or activity of the public body) together with your enabling bylaw or staff authorization	Insert the provincial or regional authority reference and program citations
(c) The title, address and business telephone of an officer who can answer questions	TrueNorth side: Privacy contact — support@truenorthcivicai.ca	Insert your Information Access and Privacy Officer name, title, address and telephone
(d) How an individual can obtain access to, or correction of, their information	Users can access and correct their own profile; institutional records are accessed through your FOI process	Insert your FOI officer contact and request channel

BEFORE GO-LIVE

Publish or update the notice of collection on the page or form where staff are introduced to the platform, and keep a dated copy with this assessment. If the purpose of collection changes, update the notice before the new use begins.

6. Security and Privacy Safeguards

Data residency	Infrastructure is deployed to GCP northamerica-northeast1 (Montréal, Canada), the only production region permitted by the platform's environment validation.
Encryption	TLS 1.3 in transit; AES-256 at rest; customer-managed encryption keys (CMEK) available for database infrastructure on qualifying plans.
PII redaction	Google Cloud DLP inspects and redacts Canadian identifiers (for example SIN, PHN, addresses and telephone or email patterns) before text reaches any AI model.
Model training	A zero-training guarantee: customer data is not used to train AI models by the vendor or its model provider.
Access control	Firebase authentication with verified government-organization email addresses, plus optional Microsoft Entra ID (Azure AD) single sign-on; role-based access (Staff, Admin, Super Admin); tenant-isolated data access enforced on every request.
Auditability	Audit logging of significant actions, and a public transparency page that reports live platform counts and data sources.
Certifications	GCP infrastructure certifications (including SOC 2 and ISO/IEC 27001) are inherited for infrastructure services; the platform does not itself hold an independent certification.

7. Retention and Disposal Schedule

The platform defaults below are the vendor-side settings. Record your public body's decision against each record type before go-live.

TABLE 3 · RETENTION SCHEDULE

Record type	Platform default	Public body decision
Chat threads	30 days, then automatic purge	[Confirm or adjust by agreement]
Uploaded documents and generated drafts	90 days, configurable	[Confirm against your records schedule]
Meeting transcripts	Per tenant configuration	[Insert]
Audit logs	Per governance requirement	[Insert]
Content at contract termination	Deleted, with written confirmation	[Confirm disposal sign-off]

Align these defaults with your own records-retention bylaw and FOI schedule. Where a record class must be retained longer than the platform default, export it to your records management system rather than relying on the platform as the system of record.

8. Residual Risks and Mitigations

The risks below remain after the safeguards in Section 6 are applied. Each is stated plainly so your privacy officer can rate it against your institution's risk tolerance.

1. Foreign jurisdiction reach — the vendor's cloud provider is headquartered in the United States, and Gemini 3.x model inference is processed by Google in US/EU multi-regions (all persistent data remains in Montréal). US legal instruments such as the CLOUD Act can theoretically reach providers headquartered in the United States. Mitigations: enforced Canadian residency for all persistent data, DLP pre-redaction before every model call, CMEK encryption where enabled, contractual data-processing terms, and 30/90-day auto-purge.
2. Content accuracy — AI-assisted summaries and drafts may contain errors. Human review checkpoints are built into workflows and staff remain accountable for outputs; cited sources link to the underlying bylaws and statutes.
3. Scope creep of use — staff may be tempted to enter personal information beyond the assessed purposes. Mitigations: tenant policy controls, FOIPPA-oriented onboarding, and DLP pre-processing redaction.
4. Vendor access — vendor staff access is restricted to support and incident investigation. Mitigations: contractual confidentiality, audit logging, and support workflows reviewed in this assessment.

> **DECISION REQUIRED**
> Residual risk accepted or not accepted: [public body to decide and document]. Record the decision, the date and the person who made it.

9. Approvals and Sign-Off

By signing, the public body records that it has reviewed this assessment, understands the identified risks, and has decided whether to proceed on the terms recorded in Section 8.

Role	Name	Signature	Date
Prepared by	[Name / title / date]		
Reviewed by — Privacy	[Name and title]		
Reviewed by — IT security	[Name and title]		
Departmental approval	[Name and title]		
Delegated decision-maker sign-off	[Name and title]		

Appendix A: Attachments

1. TrueNorth Civic AI — IT Security and Architecture Brief (companion document in this kit).
2. Sole-Source and Direct-Award Justification Memorandum (companion document in this kit, for purchasing).
3. [Optional] Vendor data-processing agreement and subscription terms.
4. [Optional] Data inventory extract or tenant configuration screenshots.

Document control: prepared by TrueNorth Civic AI. Template version 1.0; vendor facts current as of October 2026. This template supports, and does not replace, your public body's PIA process.