ONTARIO · MUNICIPAL IT REVIEW

IT Security and Architecture Brief

What a municipal IT security reviewer needs in one document: residency, encryption, identity, auditability, and the certifications TrueNorth inherits from its cloud infrastructure.

Prepared for	[Insert municipality name]
Service	TrueNorth Civic AI
Date	[Insert date]
Classification	Vendor-supplied — for review

Contents

1. Platform Overview 3
2. Canadian Data Residency 3
3. Encryption 3
4. Identity, Access and Tenancy 4
5. Privacy Engineering 4
6. Auditability and Transparency 5
7. Certifications and Compliance Inheritance 5
8. Operational Security Posture 6
9. Residual Jurisdictional Risk Statement 6
10. Contacts 7

1. Platform Overview

TrueNorth Civic AI is a software-as-a-service workspace for Canadian municipal staff: research grounded in BC statutes and municipal bylaws with source citations, document drafting, meeting transcription and minutes, multimodal uploads, and configurable workflow automation with human-in-the-loop checkpoints.

Architecture summary: Google Cloud Run services in GCP northamerica-northeast1 (Montréal); PostgreSQL with vector extensions for the retrieval corpus; Cloud Storage for documents; Vertex AI (Gemini family) for model inference; Google Cloud DLP for personal information inspection and redaction; Firebase Authentication for identity.

> **HOW TO READ THIS BRIEF**
> Each section states what is implemented, not what is planned. Where a control depends on the plan you purchase (for example customer-managed encryption keys), that dependency is stated explicitly. Anything the vendor cannot independently certify is described as inherited from Google Cloud.

2. Canadian Data Residency

Production data stores are pinned to northamerica-northeast1 (Montréal), and environment validation refuses to boot production in any other region. Grounding content — BC statutes and municipal bylaws — is ingested into the same region, as are RAG embeddings and the self-hosted transcription job. Gemini 3.x chat inference is the one exception: Google does not offer a Canada-region Gemini chat option, so these calls run through the Vertex AI global endpoint and the ML processing occurs in Google's US/EU multi-regions, per Google's published data-residency documentation and as disclosed in the pre-filled PIA. This brief, the pre-filled PIA and the procurement memorandum are supplied so your privacy and IT teams can verify rather than trust.

> **HOW TO VERIFY**
> Request the production environment configuration and region validation behaviour during onboarding, or ask for a walkthrough with your IT lead. Residency is enforced in application configuration and infrastructure deployment, not asserted only in marketing material.

3. Encryption

In transit	TLS 1.3 for all browser and API traffic; HTTPS-only endpoints.
At rest	AES-256 across Google Cloud storage services, including document storage and database volumes.
Customer-managed keys	CMEK is available on the database infrastructure for qualifying plans, allowing the public body to control key material for its own data store.
Key management	Keys are managed in Google Cloud KMS in the Canadian region; access is restricted to the platform service accounts that require it.

4. Identity, Access and Tenancy

Authentication	Firebase Authentication; accounts use government-organization email addresses with email verification. Optional Microsoft Entra ID (Azure AD) single sign-on lets Microsoft 365 work accounts sign in and be matched to your tenant by verified email domain.
Authorization	Role-based access (Staff, Admin, Super Admin). Organization (tenant) isolation is enforced on every request through tenant-aware middleware; workflow execution and document-version operations re-verify ownership at the service layer.
Administrative actions	Tenant status changes and test utilities can be restricted to Super Admins and are excluded from public routes.
Account lifecycle	Accounts are created for named staff and removed when a role ends. Where single sign-on is used, access follows your directory.

5. Privacy Engineering

DLP pre-processing	Personal identifiers are detected and redacted before text reaches an AI model.
Zero training	Customer content is not used for model training by the vendor or its model provider.
Retention	Chat threads auto-purge at 30 days; uploaded documents are retained 90 days by default (adjustable by agreement); deletion is performed on request or at contract end.
Public assistant	The marketing-site assistant is guest-accessible but strictly rate-limited, capped and restricted to static public knowledge; it does not access tenant data.

6. Auditability and Transparency

- Significant platform actions write audit records that identify the actor, the action and the time.
- Public transparency endpoints report live counts of indexed documents and grounded sources — for example the number of BC municipalities covered — rather than marketing counters.
- Infrastructure and application changes deploy automatically through CI/CD with unit-test verification.
- Production configuration and secrets are served from Google Secret Manager, not from source control.

7. Certifications and Compliance Inheritance

The platform runs on Google Cloud infrastructure whose facilities, networks and core services are covered by Google's SOC 2 Type 2 and ISO/IEC 27001 (plus 27017 and 27018) certifications. Those certifications apply to the underlying infrastructure; the application layer relies on the controls described in this brief.

The platform is engineered to align with Ontario MFIPPA expectations for public-body data handling and supplies a pre-filled PIA for your review. Your obligations under the Municipal Freedom of Information and Protection of Privacy Act remain with your municipality, and questions about how the Act applies should go to the Information and Privacy Commissioner of Ontario.

> **WHAT THIS DOES NOT CLAIM**
> TrueNorth does not hold an independent SOC 2 or ISO 27001 certification for its own application layer. Any statement that the platform is "certified" should be read as describing the inherited Google Cloud infrastructure, and your reviewer should test the application controls separately.

8. Operational Security Posture

The control summary below is the set of specifics your IT security review will want, including network egress restrictions, secrets handling and retention mechanics.

TABLE 1 · CONTROL SUMMARY

Control area	Implementation
Data residency	All primary infrastructure is pinned to GCP northamerica-northeast1 (Montréal); environment validation refuses non-Canadian production regions
Encryption in transit	TLS 1.3 for browser and API traffic; HTTPS-only endpoints; HSTS enabled
Encryption at rest	AES-256 by default across GCP storage services; customer-managed encryption keys (CMEK) on the PostgreSQL infrastructure for qualifying plans
PII redaction	Google Cloud DLP pre-processing detects and redacts Canadian identifiers (SIN, PHN, addresses, contact patterns) before AI model calls
Model data handling	Zero-training guarantee — customer content is not used to train models. Persistent data and RAG embeddings are processed and stored in Montréal; Gemini 3.x chat inference (Vertex AI global endpoint) is processed by Google in US/EU multi-regions per Google's published data-residency matrix and disclosed in the pre-filled PIA
Authentication	Firebase Authentication with verified government-organization email addresses, plus optional Microsoft Entra ID (Azure AD) single sign-on for Microsoft 365 work accounts, matched to the tenant by verified email domain
Authorization model	Roles: Staff, Admin and Super Admin; tenant isolation enforced per request; workflow execution access is re-checked at the service layer
Audit and transparency	Action audit logging; public transparency endpoints report live platform counts (indexed documents, chunks, municipalities); unit-tested security controls with CI/CD on every deploy
Secrets management	Runtime secrets served from Google Secret Manager; JWT secrets required at 32 characters or more, with production fail-fast validation
Network controls	Cloud Run with private-range VPC egress; health and liveness probes; automatic deployments under CI/CD
Retention and purge	Chat auto-purge at 30 days; documents at 90 days (configurable); deletion on request or at contract end

9. Residual Jurisdictional Risk Statement

The vendor’s cloud provider is headquartered in the United States, and Gemini 3.x model inference is processed in Google’s US/EU multi-regions; all persistent data remains pinned to the Montréal region. US legal instruments such as the CLOUD Act can in principle reach providers headquartered in the United States. Mitigations: enforced Canadian residency for persistent data, DLP pre-redaction before model calls, CMEK key control where enabled, contractual terms, and short retention cycles (30/90-day purge).

DOCUMENT THE DECISION

Municipalities should record their acceptance, or any further mitigation, of this residual risk in the PIA. The decision belongs to your municipality, not the vendor.

10. Contacts

Security and privacy	support@truenorthcivicai.ca — security questions, incident reports and disclosure inquiries.
Support	truenorthcivicai.ca — support portal and product documentation.
Response expectation	Security and privacy inquiries are acknowledged within one business day.

This brief describes the platform as operated today. It does not assert an independent certification by the vendor; inherited certifications apply to the underlying Google Cloud infrastructure.