5160 Decarie Boulevard, Suite 502
Montreal, QC, H3X 2H9 Canada
privacy@simplyvoting.com

Privacy Impact Assessment

& Re-identification Risk Assessment

Simply Voting Online Voting System – Ontario Municipal Elections

Document Version: 1.0
Date of Issue: 2026-05-25
Next Scheduled Review: 2029-05-25
Prepared by: Brian Lack, President & Data Protection Officer

1. Executive Summary

This document constitutes a combined Privacy Impact Assessment (PIA) and Re-identification Risk Assessment (ReRA) prepared by Simply Voting Inc. ("Simply Voting") in respect of its online voting system as deployed for Ontario municipal elections. It is prepared in accordance with the requirements set out in section 7.1.3.4 of CAN/DGSI 111-1:2024, the National Standard of Canada governing the implementation of online voting in Canadian municipal elections.

Simply Voting prepares this assessment as a service provider. Municipalities, as the institutions accountable under the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) and the Ontario Municipal Elections Act, 1996, remain the controllers of elector personal information. This assessment is intended to be incorporated into each municipality's broader privacy and procurement due diligence.

Key findings of this assessment:

• All personal information processed by Simply Voting in connection with Ontario municipal elections is stored and processed exclusively within Canada.

• The architecture of the online voting system enforces logical separation between elector identity and the cast ballot. By design, no persisted record links a specific elector to the content of their ballot, and the runtime application has no code path that creates such a link.

• Technical and organizational controls are independently assessed annually under a SOC 2 Type 1 examination of Simply Voting's online voting system; the underlying hosting infrastructure (Hut 8 Canada) is independently assessed under a SOC 2 Type 2 examination.

• Residual privacy risks identified in this assessment are limited in nature and are accompanied by documented mitigations. They are disclosed in Section 10 in accordance with section 7.1.3.4 (b) of CAN/DGSI 111-1:2024.

This assessment should be read in conjunction with: (a) Simply Voting's annual SOC 2 Type 1 report; (b) Simply Voting's Memorandum of Agreement and Data Processing Addendum executed with each municipality; (c) the Hut 8 Canada SOC 2 Type 2 report; (d) Simply Voting's Security Policy Manual; and (e) where applicable, the privacy and security materials of DataFix VoterView, contracted directly by the municipality. The SOC 2 reports and Security Policy Manual are available to municipal clients on request under appropriate confidentiality arrangements.

2. Scope and Exclusions

2.1 In Scope

This assessment covers:

• Simply Voting's fully managed online (internet) voting service, in which Simply Voting performs election setup, elector list ingestion, Voter Information Letter production, voting system operation, and post-election reporting under the direction of a municipal Returning Officer.

• Voter authentication by mailed Personal Identification Number (PIN) combined with date of birth as a second shared secret.

• Personal information of electors, candidates, and authorized municipal users that is collected, processed, or stored by Simply Voting in the course of delivering the online voting service for an Ontario municipal election.

2.2 Out of Scope

The following are explicitly outside the scope of this assessment:

• **Telephone (IVR) voting**. CAN/DGSI 111-1:2024 is scoped to online voting and does not extend to telephone voting. Where Simply Voting offers telephone voting as a complementary channel, it is outside the scope of this assessment. A separate description of telephone voting controls is available on request.

• **Email-based delivery of Voter Information Letters (VILs).** Email VIL is an optional notification feature used for one-off post-revision letter replacements; it does not form part of the voting transaction and is outside the scope of this assessment. A separate description of the Email VIL channel is available on request.

• **Self-service deployments**. This assessment covers only Simply Voting's fully managed service, which is the offering used for Ontario municipal elections.

• **DataFix VoterView controls**. DataFix VoterView is contracted directly by the municipality (not by Simply Voting) and is the municipality's own processor. Simply Voting integrates with VoterView via a secure two-way API; the data flow is described in Section 6, but VoterView's internal controls are addressed by DataFix and the municipality's separate contract.

2.3 Refresh Cycle

In accordance with section 7.1.3.4 (a) of CAN/DGSI 111-1:2024, this assessment will be refreshed (i) upon any material change to how personal information is collected, used, or retained by Simply Voting in delivering the online voting service, and (ii) in any event no less than once every three years. The next scheduled review is identified on the cover page.

3. System Description

Simply Voting Inc. is a Canadian company headquartered in Montreal, Quebec, providing online voting services since 2003. The Simply Voting online voting system is a multi-tenant, web-based application that allows authenticated electors to cast ballots remotely via a standard web browser. The system is delivered as a managed service in the context of Ontario municipal elections.

A typical election lifecycle proceeds as follows. The municipality establishes its list of eligible electors using DataFix VoterView. Simply Voting ingests the initial elector list by manually downloading an encrypted export from the DataFix Upload/Download portal over HTTPS, and loading it into the Simply Voting application. Thereafter, a real-time two-way HTTPS API integration with VoterView keeps the two systems in sync for the remainder of the election. Simply Voting generates a unique numeric PIN for each elector and transmits the elector data and PINs via secure file transfer protocol (SFTP) to the contracted print and mail house (Taylor-Demers, Toronto). Voter Information Letters are printed and deposited with Canada Post for distribution to electors. During the voting period, each elector authenticates to the voting system using their PIN and date of birth, is presented with the appropriate ballot for their ward and (where applicable) school board support, makes their selections, confirms, and submits. Upon submission, the encrypted ballot record is written to the Votes table in a single atomic transaction that simultaneously marks the elector's record as having voted. The Votes table record contains no reference to the elector. At the close of voting, the Returning Officer unlocks the results and Simply Voting produces the final reports. After the audit and recount retention period, election data is destroyed at the written instruction of the Returning Officer and a certificate of destruction is issued.

Detailed descriptions of the system's technical components, controls, and operational procedures are provided in Simply Voting's annual SOC 2 Type 1 report and its Security Policy Manual, available to municipal clients on request. This assessment focuses on privacy-specific analysis and references those documents where appropriate.

4. Legal Authority and Accountability

4.1 Roles

In respect of elector personal information processed in connection with an Ontario municipal election:

• The municipality is the institution accountable under MFIPPA and is the controller of elector personal information.

• Simply Voting is the processor, acting under the documented instructions of the municipality as set out in the executed Memorandum of Agreement and its Data Processing Addendum.

• DataFix is the municipality's separate processor, contracted directly by the municipality for elector list management.

4.2 Lawful Authority

The municipality's authority to collect and use elector personal information for the conduct of an election arises principally under the Ontario Municipal Elections Act, 1996, including section 42 (which authorizes alternative voting methods such as internet voting where adopted by by-law) and the elector record-keeping provisions of the Act. Simply Voting's processing is limited to that which is necessary to deliver the voting service to the municipality.

4.3 Governance and External Validation

Simply Voting maintains the following governance arrangements relevant to the protection of personal information:

• A designated Data Protection Officer (privacy@simplyvoting.com) responsible for compliance with the Data Processing Addendum and applicable data protection law.

• A documented Security Policy Manual, reviewed annually by Senior Management.

• Annual third-party SOC 2 Type 1 examination of the online voting and internet elections services system (Security, Availability, and Confidentiality trust services criteria).

• Annual TrustArc Privacy Certification.

• Daily PCI-DSS compliance scanning (Trust Guard) of production voting system servers.

• Annual third-party penetration testing (CyberHunter).

• Quarterly static application security testing (HP Fortify).

• Cyber Liability insurance covering Errors & Omissions and Privacy Breach exposures.

5. Data Inventory

The following table identifies the categories of personal information that Simply Voting collects, receives, processes, or stores in the course of delivering the online voting service for an Ontario municipal election.

Data Category	Elements	Source	Sensitivity
Elector Identity	Elector ID, full name, physical address (the voting-rights address), mailing address, ward, school board support	Municipality via DataFix VoterView	Standard PII
Date of Birth	Full DOB used as second authentication factor	Municipality via DataFix VoterView	Quasi-identifier; sensitive in re-identification context (see Section 8)
Authentication Credential	Nine-digit numeric PIN	Generated by Simply Voting; mailed to elector by Taylor-Demers via Canada Post	Sensitive (enables ballot access)
Vote-time Metadata	Voted status, vote timestamp, originating IP address, country code, browser user-agent string	System-captured at moment of vote submission and stored on the Electors record	Standard PII (links to elector identity, not ballot content)
Ballot Record	Encrypted record of elector selections, with random receipt code	Created at moment of vote submission	Sensitive content; anonymized by design (no reference to elector)
Audit / Log Data	Elector login events, ballot open / confirm / submit events; administrator actions; each with timestamp and IP address	System-generated	Standard PII (elector identity; ballot content excluded)
Candidate Information	Candidate names, descriptions, positions sought	Municipality	Public record

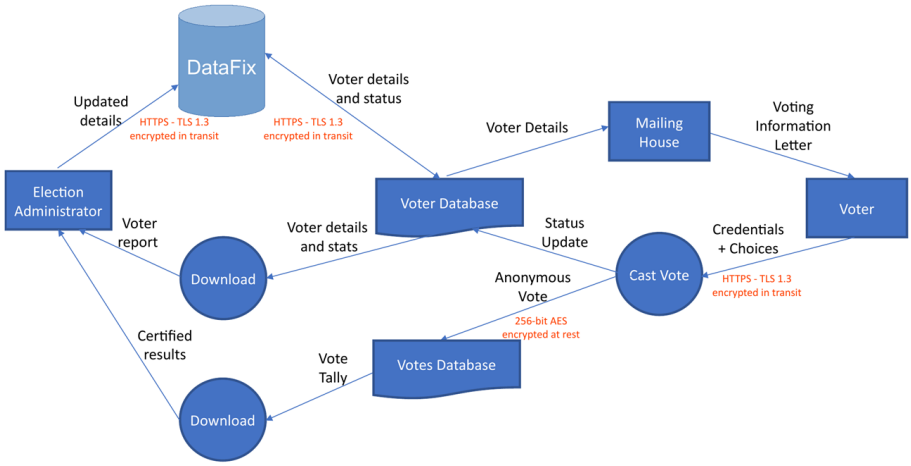
Data Category	Elements	Source	Sensitivity
Administrator Information	Name, email, phone number, role, username, hashed password, TOTP (2FA) secret	Municipality	Standard PII

Volume estimates: a representative Ontario municipality served by Simply Voting has between 5,000 and 100,000 eligible electors. Simply Voting served 50 Ontario municipal and school board elections in the 2022 cycle.

6. Data Flows and Parties

6.1 Data Flow Diagram

The following diagram depicts personal information flows among the parties involved in delivering an Ontario municipal online election at a high level. Personal information transmitted between any two parties is encrypted in transit using TLS 1.3 (or SFTP for transmission to the print and mail house). Personal information stored by Simply Voting is encrypted at rest using AES-256. The Electors table and the Votes table are two tables within the same Simply Voting database; they have no foreign key, identifier, or other association linking elector identity to ballot content (see Section 8 for detailed analysis). The diagram is a high-level representation; for the precise sequence of data movements, refer to the narrative description in Section 6.2.



6.2 Narrative Data Flow

Personal information flows through the online voting service in the following sequence:

• **Step 1 — Elector list origination**. The municipality establishes and maintains the elector list in DataFix VoterView, with which it has a direct contractual relationship. Simply Voting does not collect elector data from any other source.

• **Step 2 — Simply Voting / VoterView ingestion and synchronization**. The initial elector list is ingested by manually downloading an encrypted export from the DataFix Upload/Download portal over HTTPS and loading it into the Simply Voting application. Thereafter, a real-time two-way HTTPS API integration keeps the two systems in sync: VoterView pushes changes to elector records to Simply Voting, and Simply Voting pushes voted-status updates back to VoterView. The data exchanged is limited to elector identity, physical address, mailing address, ward, school board support, date of birth, and voting status.

• **Step 3 — PIN generation**. Simply Voting generates a random nine-digit numeric PIN for each elector. PINs are stored in association with the elector record for the duration of the election to support authentication and revisions.

• **Step 4 — Print and mail**. Simply Voting transmits elector address data and PINs to Taylor-Demers (Toronto, Canada) via SFTP for printing and Canada Post mailing. Taylor-Demers operates under a confidentiality and security regime including criminal background checks, federal Level B Enhanced clearance, and SOC 2 Type 2 attestation.

• **Step 5 — Authentication and voting**. The elector accesses the branded voting website over HTTPS/TLS 1.3 from their own device. The elector submits their PIN and date of birth. On successful authentication, the elector is presented with their ballot.

• **Step 6 — Ballot submission**. On confirmation, the application writes the encrypted ballot record to the Votes table and updates the elector's record in the Electors table to mark them as having voted, in a single atomic database transaction. The Votes table record contains only the election identifier, a random receipt code, the encryption method, and the encrypted ballot data; it does not contain any reference to the elector and does not contain a timestamp. The vote timestamp, originating IP address, country code, and browser user-agent string are captured on the elector's record in the Electors table. The voted-status update is then pushed back to VoterView.

• **Step 7 — Reporting and destruction**. At the close of voting, the Returning Officer unlocks the results. Final reports are produced and provided to the municipality. At the written request of the Returning Officer following the statutory audit and recount window (120 days post-election per Municipal Elections Act s. 88, or longer if a recount or controverted election is pending), Simply Voting destroys all election data; data is cycled out of backups approximately fifteen days thereafter. A certificate of destruction is issued.

6.3 Sub-processors and Third Parties

The following sub-processors are engaged by Simply Voting in the delivery of the in-scope online voting service to Ontario municipalities:

Sub-processor	Data Location	Activity	Safeguards
Hut 8 Canada (Mississauga, ON)	Canada	Primary cloud hosting infrastructure (production and hot-site)	SOC 2 Type 2 Master Services Agreement GDPR Adequacy Determination
Amazon Web Services Canada (Toronto, ON)	Canada (Central region)	Encrypted backup storage (S3)	SOC 2 Type 2 ISO 27001 Data Processing Agreement

Sub-processor	Data Location	Activity	Safeguards
			Standard Contractual Clauses
Tresorit AG (Zurich, Switzerland)	Canada (customer-selected residency under Tresorit Enterprise)	Encrypted file transfer and storage	ISO 27001 Data Processing Agreement GDPR Adequacy Determination Customer-selected Canadian data residency
Taylor-Demers (Toronto, ON)	Canada	Voter Information Letter printing and Canada Post mailing	SOC 2 Type 2 Government of Canada Level B Enhanced security clearance Confidentiality agreements

6.4 DataFix VoterView

DataFix VoterView is the municipality's electoral data management platform and is contracted directly by the municipality, not by Simply Voting. DataFix is the municipality's own processor under the municipality's separate contract. Simply Voting integrates with VoterView on the municipality's instruction for the purpose of receiving the elector list and synchronizing voting status. DataFix is not a Simply Voting sub-processor and is not included in the table above; municipalities should consult DataFix and their VoterView contract for the privacy and security posture of that system.

6.5 Candidate View (Optional Feature)

Candidate View is an optional feature in which a municipality may grant individual candidates real-time, read-only access to a subset of the elector list during the voting period. This serves a legitimate electoral purpose: candidates are entitled under the Municipal Elections Act to elector information for the purpose of canvassing and verifying voter participation, and Candidate View provides this access through a more secure delivery mechanism than emailing CSV files. Where the feature is enabled, the following applies:

• Each candidate accesses the Simply Voting Election Manager through a dedicated login protected by a password and TOTP-based two-factor authentication.

• The data visible to a candidate is limited to elector name, physical address, and voted status (whether or not the elector has voted).

• Where the election is divided by ward, each candidate sees only the electors of the ward in which they are running.

• Candidates do not see PINs, dates of birth, mailing addresses, ballot content, or any other data field.

• Candidate access is logged and is automatically terminated at the close of the voting period.

• Municipalities that prefer to use the equivalent feature in VoterView, or to provide candidates with paper lists, may decline to enable Candidate View.

6.6 Cross-border Data Flows

Within the scope of this assessment, no personal information is transmitted to, processed in, or stored in a jurisdiction outside Canada. All in-scope sub-processors are either Canadian or operate under a customer-selected Canadian data residency configuration.

7. Privacy Principles Assessment

This section assesses Simply Voting's processing of personal information against the fair information practices that underpin Canadian privacy law generally and MFIPPA in particular. Where the corresponding control is described in greater technical detail in Simply Voting's SOC 2 Type 1 report or Security Policy Manual, those documents are referenced.

7.1 Accountability

Simply Voting has designated a Data Protection Officer responsible for compliance with the Data Processing Addendum and applicable privacy law. The DPA between Simply Voting and the municipality documents the parties' respective responsibilities. Annual third-party SOC 2 and TrustArc examinations provide independent assurance.

7.2 Identifying Purposes

Personal information is collected from electors for the sole purpose of conducting the online voting service for which the municipality has engaged Simply Voting. Purposes are documented in the Memorandum of Agreement, the Data Processing Addendum, and the Simply Voting Privacy Policy.

7.3 Consent

Under MFIPPA and the Municipal Elections Act, the municipality's collection and use of elector personal information for the conduct of the election is lawfully authorized; consent of the individual elector is not the operative basis. Simply Voting's processing is on the documented instruction of the municipality.

7.4 Limiting Collection

Simply Voting collects only the personal information that is required to deliver the online voting service, as set out in Section 5. No additional data elements beyond those required by the election configuration are collected. The Data Processing Addendum obligates the municipality not to transfer to Simply Voting any personal information beyond that needed to deliver the services.

7.5 Limiting Use, Disclosure, and Retention

Personal information is processed only for the purpose of delivering the online voting service. Election data is retained for the statutory audit and recount window (120 days following election day, per s. 88 of the Municipal Elections Act, or longer if a recount or controverted election is pending) and is destroyed thereafter on the written instruction of the Returning Officer. A certificate of destruction is issued.

7.6 Accuracy

Elector record accuracy is the responsibility of the municipality, managed via DataFix VoterView, including a defined revisions process to correct errors before and during the voting period. The two-way real-time sync between VoterView and Simply Voting ensures that corrections made in VoterView are reflected in Simply Voting without delay.

7.7 Safeguards

Simply Voting implements technical and organizational controls including: AES-256 encryption of data at rest; TLS 1.3 in transit; role-based access controls with regular access reviews; multi-factor authentication for administrative access; network segmentation behind FortiGate UTM firewalls with intrusion detection; web application firewall (WAF) protection; brute-force protection on the voting interface; advanced distributed denial of service (DDoS) mitigation via NETSCOUT Arbor at the ISP level; centralized log aggregation; daily file integrity scanning on production servers; an hourly automated check that the application code present on each production web server matches the Git master branch, with alerts on any mismatch; annual third-party penetration testing; quarterly static code analysis; security incident response procedures; and personnel confidentiality obligations. These controls are described in detail and independently assessed in the annual SOC 2 Type 1 report and documented in the Simply Voting Security Policy Manual.

7.8 Openness

Simply Voting maintains a public Privacy Policy at simplyvoting.com. This PIA is provided to each Ontario municipal client. The SOC 2 Type 1 report, the Hut 8 SOC 2 Type 2 report, the Security Policy Manual, and other third-party audit reports are available to municipal clients on request under appropriate confidentiality arrangements.

7.9 Individual Access

Because Simply Voting acts as a processor under the municipality's instruction and has no direct relationship with individual electors, requests from electors for access to or correction of their personal information are directed to the municipality (the controller). Simply Voting provides the municipality with self-service tools and, on request, professional services to fulfill such requests within the timeframes required under MFIPPA.

7.10 Challenging Compliance

Privacy complaints may be directed to privacy@simplyvoting.com. Unresolved complaints concerning Simply Voting's privacy practices may be escalated via TrustArc's third-party dispute resolution facility. Municipal-level privacy complaints are subject to the jurisdiction of the Information and Privacy Commissioner of Ontario.

8. Re-identification Risk Assessment

This section constitutes the Re-identification Risk Assessment required under section 7.1.3.4 of CAN/DGSI 111-1:2024. The central question addressed is: given the personal information held by Simply Voting in connection with an Ontario municipal election, can any held dataset, alone or in combination, be used to link a specific elector to the content of their cast ballot?

8.1 Datasets Held by Simply Voting

In the course of conducting an online voting election, Simply Voting holds the following datasets:

• **Electors table:** elector identity, physical and mailing addresses, ward, school board support, date of birth, PIN (stored in the password field), voted status, and — once the elector has voted — the vote timestamp, originating IP address, country code, and browser user-agent string.

• **Votes table**: the encrypted ballot records. The Votes table contains only four fields: election identifier, a random five-character receipt code (for Ontario municipal elections), the encryption method, and the encrypted ballot data. The primary key is the composite of election identifier and receipt code.

• **Election log**: system events including elector login, ballot open, ballot confirmation, ballot submission, administrator actions, and revisions actions, each with timestamp and originating IP address.

8.2 Potential Linking Attributes

The attributes by which an actor might in principle attempt to link an elector to a specific ballot record are limited:

• The Votes table contains no submission timestamp, no auto-incrementing identifier, and no reference to the elector. The composite primary key (election identifier plus random receipt code) is used by the database engine to order physical row storage, so insertion order cannot be inferred from the on-disk row order.

• The Electors table includes a receipt field that could in principle be populated to link to the Votes table. For Ontario municipal elections, however, accounts are configured such that this receipt field is never populated by the application. The Simply Voting application has no code path that writes the receipt value into the Electors table for these elections.

• Vote timestamps are recorded on the elector's record in the Electors table, but not in the Votes table itself — so timestamps exist on the identity side, with no corresponding timestamp on the ballot side against which to correlate.

8.3 Architectural Separation

The Electors table and the Votes table reside in the same Simply Voting database, but the architecture prevents linkage by design through three reinforcing mechanisms:

• Schema separation. The Votes table has no foreign key, identifier, or other field referencing the Electors table. The only foreign key on the Votes table is to the Elections table (i.e., which election the vote belongs to).

• No timestamp on the Votes table. Vote timestamps are recorded only on the elector's record in the Electors table. The Votes table itself contains no time-of-vote attribute.

• Insertion-order obscurity. The Votes table's primary key is the composite of election identifier and a random receipt code. Because the database stores InnoDB table rows ordered by primary key, and the receipt is random, the physical row order in the Votes table does not reflect the order in which ballots were submitted.

The act of voting writes the ballot record and updates the elector's voted status in a single atomic transaction, but the two writes do not establish a referential link. Following ballot submission, there exists no persisted artifact within the Simply Voting system that connects a specific elector to a specific ballot record.

8.4 Residual Re-identification Risk

Notwithstanding the architectural separation, the following residual risks are acknowledged for completeness:

• **Insider correlation attempt against vote-time metadata**. Although the Votes table itself contains no timestamp, the Electors table records the moment at which each elector voted. A privileged insider with read access to the Electors table and to the application logs could in principle attempt to correlate elector vote-times with log entries documenting ballot submissions. Because the receipt code generated for each ballot is random and is not stored on the elector record (see Section 8.2), this correlation does not yield a direct mapping; it would at best narrow a candidate set within the time window of an elector's session. In an election with meaningful turnout and concurrency, this does not identify any specific elector-ballot pairing. The risk is further mitigated by role-based access controls, regular access reviews, comprehensive logging of administrator actions, and the personnel confidentiality and code-of-conduct obligations described in the Security Policy Manual and SOC 2 report.

• **Runtime application linkage**. Although no persisted record links elector identity to ballot content, the running voting application necessarily handles both in process memory during the brief authentication-and-submission transaction. A privileged party with the ability to introduce malicious code into the production application could, in principle, attempt to capture that linkage at runtime. The following layered controls mitigate this risk: (i) all source code changes pass through a controlled Software Development Life-Cycle that requires pull request, peer review, security audit, and QA testing by a separate reviewer before promotion to production (Security Policy Manual, SDLC Policy); (ii) only the President or IT Director may migrate code to the production environment, and only from the master Git branch; (iii) quarterly third-party static code analysis (HP Fortify); (iv) annual third-party penetration testing (CyberHunter); (v) an automated process compares the application code present on each production web server against the master Git branch on an hourly basis and alerts on any mismatch, providing near-real-time detection of unauthorized code modification; and (vi) generative AI tools may not be used to write or modify production voting system code without human review (Acceptable Use Policy).

• **Date of birth as a quasi-identifier in small electorates**. In a small municipality, an individual elector's date of birth may be unique within the electorate. An observer who learns from public sources (e.g., social media, obituaries) that a known individual has a specific date of birth, and who later obtains some attribute of that elector's vote, could in principle attempt to combine the two. The risk is materially limited by the following: (i) date of birth is stored on the Electors table only and is never stored, exported, or otherwise associated with the Votes table or with published election results; (ii) date of birth in the Simply Voting system functions as a shared-secret authentication factor used at the moment of login, not as a published quasi-identifier; and (iii) there is no published or routinely accessible dataset of 'who voted for whom' against which a DOB-based lookup could be performed, because no such dataset exists. The relevant analogous risk — an attacker using a known DOB to impersonate an elector and cast a fraudulent ballot — is an electoral-fraud risk rather than a re-identification risk, and is addressed by the PIN as the primary authentication factor.

• **Candidate View access (where enabled)**. Where the municipality enables Candidate View (see Section 6.5), each candidate is able to observe the voted status of electors within their ward in real time. A candidate observing that a specific named elector has voted is not learning the content of that elector's ballot; the information disclosed is voting participation only. This is the same information that would be disclosed by the equivalent VoterView feature, paper poll-book inspection, or any other lawful candidate access to the elector list. Disclosure is mitigated by per-candidate login, two-factor authentication, ward scoping, comprehensive logging of candidate access, and contractual confidentiality obligations imposed by the municipality on candidates.

• **Small-ward disclosure in published results**. Where a ward contains a very small number of electors, aggregate results reporting may indirectly disclose the votes of identifiable individuals. This is an inherent property of any electoral system (including paper ballots) and is addressed by the municipality's election design choices rather than by the voting system itself.

8.5 Conclusion

The residual re-identification risk associated with Simply Voting's online voting system is assessed as **very low**. The combination of architectural separation between elector identity and ballot content, layered controls on the application code that processes both at runtime, and the access and logging controls applicable to administrative roles, renders the practical possibility of linking a specific elector to specific ballot content negligible in normal operating conditions.

9. Risk Register

The following risks have been identified in connection with the processing of personal information through the Simply Voting online voting system. Each is rated for likelihood and impact, with documented mitigations and residual risk.

Risk	Likelihood	Impact	Mitigations	Residual Risk
Insider misuse of administrative access	Low	High	Role-based access; quarterly access reviews; 2FA required; comprehensive immutable logging; personnel confidentiality obligations; SOC 2 Type 1 attestation of access controls; ballot/voter separation prevents direct join.	Low
Unauthorized code modification on production servers	Very Low	High	Restricted prod deployment (President or IT Director only); SDLC requires pull request, peer review, security audit, and separate QA reviewer; hourly automated Git master vs. production code drift detection with alerting; daily file integrity scanning.	Very Low
Interception of voter credentials (PIN) in mail	Low	Medium	Security-lined #10 double-window envelopes; second factor (DOB) required; lost-letter revisions process invalidates old PIN; stolen-letter procedure with police notification; brute-force protection on login.	Low
Mailing house compromise (Taylor-Demers)	Very Low	High	Government of Canada Level B Enhanced clearance; SOC 2 Type 2 attestation; criminal background checks; physical access controls; confidentiality agreements; data transmitted only via secure encrypted channel.	Very Low
Credential brute force / automated guessing	Medium	Low (one ballot at most)	Automatic CAPTCHA trigger after repeated failed attempts by Elector ID, PIN, or IP; DOB second factor required; comprehensive logging and Suspicious Activity Reports; Returning Officer can block IPs and PINs in real time.	Low

Risk	Likelihood	Impact	Mitigations	Residual Risk
DDoS attack on voting system	Medium	Medium (availability)	NETSCOUT Arbor DDoS mitigation at ISP level (always-on); redundant Anycast DNS; hot-site disaster recovery in separate geographic region; tested annually under load.	Low
Application or infrastructure vulnerability exploited	Low	High	Annual penetration testing (CyberHunter); quarterly static code analysis (HP Fortify); daily PCI scanning (Trust Guard); secure SDLC with security review of all changes; WAF; hardened servers; Open Web Application Security Project (OWASP) guidelines.	Low
Sub-processor data breach	Low	Medium-High	All in-scope sub-processors are Canadian or operate under Canadian residency; each has SOC 2 Type 2 or equivalent attestation; contractual flow-down of data protection obligations; documented incident notification.	Low
Candidate misuse of elector list view (Candidate View, where enabled)	Low	Low-Medium (voting participation only; not ballot content)	Per-candidate login with TOTP 2FA; ward scoping limits visible electors; read-only access to name, physical address, voted status only (no PIN, DOB, mailing address, or ballot content); access logged; auto-terminates at close of voting; municipality's contractual confidentiality obligations on candidates; equivalent risk exists for paper poll-book and VoterView alternatives.	Low
Voter device compromise (malware on voter's own computer)	Low-Medium	Low (one voter)	Outside vendor control; mitigated in part by optional cast-as-intended verification via QR code (DGSI 111-1 s. 6.2.5); brute-force and second-factor controls limit credential reuse.	Medium (residual)

10. Residual Risks Disclosed to Municipalities

In accordance with section 7.1.3.4 (b) of CAN/DGSI 111-1:2024, Simply Voting discloses the following residual privacy risks to municipal election administrators for their consideration in adopting and operating the online voting service:

• **Voter device security is outside vendor control**. The security of the device the elector uses to vote (personal computer, phone, tablet) is the responsibility of the elector. Where a voter's device is compromised by malware, the confidentiality or integrity of that voter's ballot could in principle be affected. This risk is partially mitigated by the optional cast-as-intended verification feature, which allows the voter to confirm their vote was recorded as intended using a separate device.

• **Insider correlation against vote-time metadata**. While the Votes table contains no timestamp and no reference to the elector, the Electors table records the moment at which each elector voted. A privileged insider could in principle attempt to correlate elector vote-times with application log entries, although no direct mapping is recoverable in this manner. Mitigations are documented in Section 8.4. The residual practical possibility of identifying any specific elector's ballot is negligible in elections of typical size and concurrency.

• **Runtime linkage by unauthorized code modification**. The voting application necessarily handles elector identity and ballot content in process memory during the moment of vote submission. A party able to introduce unauthorized code into the production system could in principle attempt to capture that linkage at runtime. This residual risk is mitigated by the multi-layered controls described in Section 8.4, including restricted production deployment authority, peer-reviewed code changes through the documented SDLC, third-party static analysis and penetration testing, and an hourly automated check that the application code on each production server matches the Git master branch.

• **Date of birth as a quasi-identifier in small electorates**. In a small municipality, an elector's date of birth may be unique within the electorate. Date of birth is used in the Simply Voting system as a shared-secret authentication factor; it is stored only on the Electors record and is never stored alongside or linked to the Votes table, nor is it included in published election results. There is therefore no dataset against which a known DOB could be combined to identify how a specific elector voted. The related risk — use of a known DOB combined with a stolen PIN to impersonate an elector — is an electoral-fraud risk rather than a re-identification risk and is addressed by the PIN as the primary authentication factor.

• **Candidate observation of voting participation (Candidate View, where enabled)**. Where a municipality enables Candidate View, candidates can observe in real time which electors in their ward have voted. The information disclosed is voting participation only; the content of ballots is never visible. The same disclosure exists in the equivalent VoterView feature and in any paper poll-book delivered to candidates. Mitigations are documented in Sections 6.5 and 8.4.

• **Small-ward disclosure**. Where a ward contains a very small number of electors, aggregate results reporting may indirectly disclose the votes of identifiable individuals. This is an inherent property of any voting system and is addressed by the municipality's election design (e.g., result aggregation thresholds), not by the online voting system itself.

• **Limitations of SOC 2 Type 1**. Simply Voting's SOC 2 attestation is a Type 1 (design of controls as at a point in time), refreshed annually. It does not provide operating-effectiveness assurance over a period. The underlying hosting infrastructure (Hut 8 Canada) is independently attested under SOC 2 Type 2. Municipalities requiring Type 2 assurance over Simply Voting's own operations may wish to consider this in their procurement evaluation.

• **Optional anti-fraud tracking cookie**. An optional anti-fraud tracking cookie is available that, if enabled at the Clerk's discretion, would be associated with the elector's identity (and is therefore inconsistent with the recommendation in section 4.2.2 of CAN/DGSI 111-1:2024). This feature is disabled by default and is enabled only at the explicit instruction of the Clerk.

Each of these residuals is documented so that municipalities can make an informed accountability determination in respect of their own MFIPPA obligations.

11. Conclusion and Maintenance Commitment

Simply Voting's online voting system, as configured for Ontario municipal elections, processes elector personal information under a clearly defined controller-processor relationship with the municipality, with data stored and processed exclusively in Canada and with architectural separation between elector identity and ballot content reinforced by layered controls at the application runtime layer. The residual privacy and re-identification risks identified in this assessment are limited in nature and are accompanied by documented mitigations and external validation.

In accordance with section 7.1.3.4 (a) of CAN/DGSI 111-1:2024, this Privacy Impact Assessment and Re-identification Risk Assessment will be refreshed:

- upon any material change to the way in which personal information is collected, used, or retained in the delivery of the online voting service; and
- in any event, no less than once every three years.

Privacy inquiries, requests for the SOC 2 reports or Security Policy Manual, or requests for supplementary information should be directed to:

Brian Lack, President & Data Protection Officer

Simply Voting Inc.

5160 Decarie Boulevard, Suite 502, Montreal, QC H3X 2H9, Canada

privacy@simplyvoting.com

Appendix A – Reference Documents

The following documents are referenced in this assessment. Items marked as available on request are provided to municipal clients under appropriate confidentiality arrangements upon written request.

• Simply Voting SOC 2 Type 1 report, most recent annual examination (available on request).

• Simply Voting Security Policy Manual, current version (available on request).

• Hut 8 Canada SOC 2 Type 2 report covering the underlying hosting infrastructure (available on request).

• Taylor-Demers SOC 2 Type 2 report (available on request).

• AWS Canada SOC 2 Type 2 report covering the encrypted backup storage service (publicly available).

• Simply Voting Memorandum of Agreement, Data Processing Addendum, Terms of Service, and Privacy Policy.

• Annual penetration test report, CyberHunter (available on request).

• PCI compliance scan reports, Trust Guard (available on request).

• TrustArc Privacy Certification.

• WCAG 2.2 AA Accessibility Conformance Report (VPAT).

Appendix B – Legislative & Standards References

• CAN/DGSI 111-1:2024 — Online Electoral Voting — Part 1: Implementation of Online Voting in Canadian Municipal Elections.

• Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), R.S.O. 1990, c. M.56.

• Municipal Elections Act, 1996, S.O. 1996, c. 32, Sched., in particular ss. 42 (alternative voting methods) and 88 (retention of election materials).

• Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, c. 5.

Appendix C - Glossary

• **Controller**: the party that determines the purposes and means of processing personal information. For Ontario municipal elections, the municipality.

• **Processor**: a party that processes personal information on behalf of the controller. For the online voting service, Simply Voting.

• **PIA**: Privacy Impact Assessment.

• **ReRA**: Re-identification Risk Assessment.

• **VIL**: Voter Information Letter — the document, mailed to each elector, containing voting instructions and the elector's PIN.

• **PIN**: Personal Identification Number — a randomly generated nine-digit numeric code used as the primary authentication credential.

• **DGSI**: Digital Governance Standards Institute (formerly CIO Strategy Council / CIOSC). The Canadian Standards Development Organization that published CAN/DGSI 111-1:2024.

• **MFIPPA**: Municipal Freedom of Information and Protection of Privacy Act (Ontario).

• **SDLC**: Software Development Life-Cycle. Simply Voting's SDLC Policy is documented in the Security Policy Manual.