Integrated Electronic Voting Solutions For Municipal Voting Events

Simply Voting Security & Reliability Information

Date: January 2026

For more information contact:
info@simplyvoting.com

Security Overview

Simply Voting Inc. provides an Internet & Telephone Voting System for Municipal Elections. The Simply Voting system is secure and protects the secrecy of your vote.

Secret Ballot

Simply Voting is designed to protect the secrecy of your ballot, in the same way as a traditional paper election.

When you submit your ballot, your voting choices are encrypted and stored separately from your personal information. Once stored, there is no way for election officials, municipal staff, Simply Voting employees, or any other person to determine how you voted.

Election officials can see that you have participated in the election, along with administrative details such as the time you voted and the IP address used, but they cannot see the contents of your ballot.

As with all elections, whether conducted on paper or electronically, ballot secrecy depends on the integrity of the election process and systems. Simply Voting uses multiple layers of security controls to protect the system during voting and to prevent unauthorized access or interference.

One Person One Vote

Only registered voters on the municipal list of electors will be authorized to access a ballot. Once you vote, using either internet or telephone, you are “crossed off” the list and cannot vote again. Even if you try to vote using several devices at the same time, the system will only accept one single ballot from each voter.

Protection Against Computer Hackers

Simply Voting is an expert in internet security and goes to great lengths to protect the voting system. All communications between your computer and the voting website are encrypted to ensure confidentiality. The internet ballot is tamperproof and there are multiple layers of security to protect the servers against attacks.

Protection Against Imposters

To vote, you will need to enter a password. Every password is at minimum a nine-digit numeric PIN that will be mailed to each voter in a Voter Information Letter prior to the "Voting Period". These PINs are randomly generated by Simply Voting and are sent securely to the mailing house, a reputable electoral communications company that prints the letters, machine folds them in security-tinted envelopes and mails them directly to voters using Canada Post. As an added security measure, voters will also be required to enter their date of birth to complete the voting procedure. Therefore, if your Voter Information Letter ends up in the wrong hands, another person will not be able to cast your vote without your PIN and your date of birth.

Technical Information

Top-Notch Security

Simply Voting was designed from the ground-up to minimize the risk of electoral fraud or breach of secrecy:

- Voters who bypass authentication or have already voted are denied access to the ballot.
- One-vote-per-voter is guaranteed by marking electors as voted and storing the vote in a single transaction. Even if a voter submits the ballot simultaneously on several devices, this technology guarantees that only one vote is accepted.
- Ballots are rigorously checked for validity before being accepted.
- All administrator and voter activity is recorded with timestamp and IP address in an immutable log.
- Communication between the voter's computer and our website is encrypted with *TLS 1.3* and strong cipher suites to protect against current and future encryption attacks.
- The entire voting system database is encrypted at rest using AES-256 encryption.
- Our servers are "hardened" and are subjected to daily *Trust Guard* PCI Compliance security scans.
- Our voting system is regularly subjected to penetration tests by *CyberHunter* and source code security audits by *HP Fortify*.
- Simply Voting adheres to guidelines established by the *Open Web Application Security Project*.
- Any change to the voting system must pass an internal security review before going live.
- All staff workstations are kept up-to-date and protected by access password, firewall, anti-virus, anti-spamware and disk encryption.
- We authenticate our emails with DomainKeys Identified Mail and the Sender Policy Framework to protect voters from phishing attacks.
- Our servers are protected by a very powerful firewall, FortiGate Unified Threat Management, which includes an Intrusion Detection System (IDS) and a redundant firewall on hot standby. Webservers are further protected by the ModSecurity Web Application Firewall (WAF).

- Network access is protected by a Virtual Private Network (VPN) and Two-Factor Authentication (2FA).
- Simply Voting uses an automated and always-on solution built on NETSCOUT Arbor technology to protect against Denial of Service (DoS) attacks at the internet service provider (ISP) level before they reach our infrastructure.
- We use redundant *Anycast DNS* deployments which protects against DNS-based DDoS attacks.

Security vulnerabilities can be reported through our Vulnerability Disclosure Policy, which supports coordinated disclosure consistent with ISO/IEC 29147.

Brute Force Attacks

Simply Voting's defense against a brute-force attack (automated password guessing) is triggered when there are 10 strikes within the last 15 minutes. A strike is an incorrect login based on same Elector ID, the same PIN or the same IP address / phone number. When our brute force defense triggers on the internet voting system, the voter must complete a captcha to submit their credentials. Account lockouts are not used - they could be engineered as a denial-of-service attack vector.

Fully Hosted & Reliable

Don't worry yourself about servers, IT staff, installing software or taking backups. Simply Voting gives you instant access to the latest technology and is ready to process millions of votes around the clock.

Our online voting system is hosted in data centres operated by Hut 8 Canada, a professional cloud and colocation provider. These facilities are operated in accordance with SOC 2 Type II standards, are designed to Uptime Institute Tier III standards, and feature fault-tolerant infrastructure with redundancy across power, cooling, and network connectivity to ensure high availability and reliability. Physical access to the data centres is strictly controlled and continuously monitored. This hosting environment is designed to provide a stable, secure foundation for elections, even during periods of peak system usage.

Simply Voting uses third party offsite monitoring tools to automatically monitor key “vital signs” of our voting system 24×7 and a technical staff member is immediately notified of any anomaly. Simply Voting maintains a Disaster Recovery Plan as well as a Hot Site at a backup data center in a different geographical area. The Hot Site is synchronized with the primary data center using remote database replication. Should the primary data center experience an outage, we have the capability of quickly redirecting traffic of the entire voting system to the Hot Site, minimizing disruption to ongoing elections and avoiding any loss of data. You can rest assured that your election is always protected and available in the case of a disaster.

For telephone voting, Simply Voting uses Twilio as the interactive voice interface layered on top of our

online voting system. Twilio is a well-established cloud communications platform with a globally distributed, fault-tolerant infrastructure designed for high availability and reliability. Its systems are built with redundancy at every level and have been proven at scale through billions of calls worldwide. Twilio operates under internationally recognized security standards, including ISO 27001 and SOC 2 Type II, and applies strong controls to protect applications and data. The platform automatically scales to meet demand, eliminating busy signals even during peak voting periods.

Backups

In addition to the real-time connectivity between the two servers, every 20 minutes a full backup is taken of the entire voting system, encrypted using AES 256, and then uploaded to Amazon S3 cloud storage in the Canada (Central) region.

Load Testing

To confirm that the voting system has adequate capacity for upcoming projects, Simply Voting conducts regular scripted load testing with a cloud-based solution for mimicking human traffic.

Confidentiality

Simply Voting takes secrecy of the vote very seriously. Votes are stored without any information that could be traced to an elector, so it is logically impossible for election organizers or even the Simply Voting system administrators to determine what a particular voter has voted. We never make use of voter information for anything other than voting and never share such information with third parties. Our privacy policy (available on the Simply Voting website) and voting system have been independently certified by TRUSTe for compliance with their Privacy Certification and Trusted Cloud requirements. Furthermore, Simply Voting is compliant with PIPEDA as well as PIIDPA as well as MFIPPA All related data is the property of the Municipality and, in accordance with legislation, is not transmitted or stored outside of Canada.

SOC 2 Compliance

Simply Voting is SOC 2 Type 1 compliant. The SOC 2 is a widely recognized auditing standard issued by the American Institute of Certified Public Accountants (AICPA). An auditor's report details a service provider's ability to offer adequate controls and safeguards when they host or process data belonging to their customers. The audit focuses heavily in the areas of security, availability and confidentiality. It addresses important topics such as backup and recovery, computer operations, and human resources. The data centers where Simply Voting servers are located are similarly

SOC 2 Type 2 compliant. This attestation is an independent validation of the quality, integrity and reliability of Simply Voting's infrastructure and services.

Advanced DDoS Protection Service with NETSCOUT Arbor

Denial-of-service (DoS) attacks are on the rise and have evolved into complex and disruptive security challenges for organizations of all sizes. Although DoS attacks are not a new phenomenon, the methods and resources available to conduct and disguise them have advanced significantly, including large-scale distributed (DDoS) and distributed reflector (DRDoS) attacks.

Simply Voting uses an advanced DDoS protection service built on NETSCOUT Arbor technology and delivered through our hosting provider at the internet service provider (ISP) level. This service continuously monitors traffic destined for Simply Voting's systems and is designed to detect and mitigate high-volume floods and other denial-of-service attacks before they reach our infrastructure.

Key features of this carrier-grade protection include automated, behaviour-based detection informed by global threat intelligence; protection against volumetric, protocol, and application-layer DDoS attacks; and the ability to mitigate encrypted traffic floods without requiring access to encryption keys or introducing latency during normal operation. This approach is widely used by internet service providers and large enterprises to protect critical online services.

Simply Voting benefits from an always-on, network-layer protection model that operates upstream of our infrastructure. All inbound traffic to our routed IP address space is continuously analyzed and, when necessary, automatically mitigated within the provider's network. This design does not rely on manual intervention, traffic redirection, or DNS changes during an attack, and ensures that legitimate users can continue to access the platform even during large-scale denial-of-service events.

HUT 8

Mississauga Data Centre (FTB) — Tier III

As Hut 8's flagship facility in Eastern Canada, the Mississauga Data Centre is designed to Uptime Institute Tier III standards to provide enterprise grade system availability and resiliency. The data centre space resides on the second floor of a complex, designed and constructed by Blackberry, providing state-of-the-art design elements not found in similar facilities, including an indoor generator facility located near the data centre building for added redundancy. All power, cooling, and

connectivity infrastructure elements are built with 2N redundancy to provide fault tolerance to the entire system.

The Facility

Power

Distribution

- 4 MW designed power capacity
- In-row Remote Power Panels (RPPs) to allow for more efficient power monitoring and distribution
- 2N back-up power infrastructure
- Two dedicated municipal hydro substations
- A and B side power in every cabinet
- 208V Single or 3-Phase, 120V Single Phase available

Generators

- Ten 600kW generators (6,000 kW total) supplying backup power to the complex
- N+1 generator redundancy
- On-site fuel capacity provides >12 hours run time at full load (based on current capacity)
- Fuel capacity – 48,000 (L) capacity

UPS system

- 900kW UPS each for A and B side power
- Clean power supplied by double conversion UPS
- 2N UPS redundancy

Connectivity

- Carrier-neutral facility
- Diverse building fibre entrances
- Redundant connectivity between other data centres
- Internet transit from multiple providers including:
    - Bell
    - Zayo
    - Rogers
    - TeraGo

Cooling system

Chillers

- Fourteen 30-tonne CRAC units, supporting >1MW IT load in a N+1 configuration
- Independent air-cooled rooftop cooling unit

Cooling system design

- Hot aisle/cold aisle airflow configuration
- Chilled water towers and closed glycol loop

Compliance and certifications

Security and monitoring

- 24/7 video monitoring and surveillance by Network Operations Centre
- Multi-factor access authentication (access card and biometric)

Kelowna Data Centre (LEP) — Tier III

As Hut 8's flagship facility in Western Canada, the Kelowna Data Centre is designed to Uptime Institute Tier III standards to provide enterprise grade system availability and resiliency. It is strategically located in the south-central region of British Columbia, with one of the lowest geographic risk profiles in North America. All power, cooling, and connectivity infrastructure elements are built with N+1 and 2N redundancy to provide fault

tolerance to the entire system. Our Kelowna Data Centre is powered by 95% renewable energy via hydroelectricity.

The Facility

Power

Distribution

- 6 MW designed capacity
- 2N+1 back-up power infrastructure, from ring bus substations leading to the complex
- A and B side power in every cabinet
- 208V Single or 3-Phase, 120V Single Phase available

Generators

- Two 1,500kW generators (3,000 kW total) supplying backup power to the facility
- N+1 generator redundancy
- On-site fuel capacity provides >29 hours run time at full load (based on current capacity)
- Fuel capacity – 24,000 (L)

UPS system

- 1,000kW UPS each for A and B side power
- N+1 UPS redundancy

Connectivity

- Carrier-neutral facility
- Diverse building fibre entrances
- Redundant connectivity between other data centres
- Internet transit from multiple providers including:
    - Shaw
    - Telus
    - Zayo
    - TeraGo

Cooling system

Chillers

- Two 200-tonne Chillers, supporting >1 MW IT load at capacity
- N+1 Cooling redundancy
- ‘Free cooling’ capabilities during winter months due to region’s climate

Cooling system design

- Cold aisle containment configuration
- Chilled water system closed loop

Compliance and certifications

Security and monitoring

- 24/7 video monitoring and surveillance by Network Operations Centre
- Minimum video retention capable of 90+ days
- Exterior and interior surveillance
- Multi-factor access authentication (access card and biometric)