

Voting System Security Overview

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 Prevention System (IPS) 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 DoS attacks.

CONFIDENTIAL AND PROPRIETARY



Scan
for more
information



info@simplyvoting.com



1 (800) 585-9694



www.simplyvoting.com



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 24x7 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.

CONFIDENTIAL AND PROPRIETARY



Scan
for more
information



info@simplyvoting.com



[1\(800\)585-9694](tel:1(800)585-9694)



www.simplyvoting.com



Confidentiality



Simply Voting takes secrecy of the vote very seriously. It is impossible for election organizers to determine what a particular voter has voted as the results are anonymous. All voter information is removed from our servers if you choose to have the election deleted. 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.

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.

CONFIDENTIAL AND PROPRIETARY



Scan
for more
information



info@simplyvoting.com



[1 \(800\) 585-9694](tel:1(800)585-9694)



www.simplyvoting.com



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.

For more information, please write to info@simplyvoting.com

CONFIDENTIAL AND PROPRIETARY



Scan
for more
information



info@simplyvoting.com



[1\(800\)585-9694](tel:1(800)585-9694)



www.simplyvoting.com