OneFeather

Online Voting Security

Frequently Asked Questions

Protecting Your Vote

How secure is your online voting system?

Security is our top priority. Our system is built with multiple layers of protection, including end-to-end encryption, secure access controls, robust user verification, and advanced threat detection. We also maintain **SOC 2 certification** through Prescient Security, ensuring we follow strict security policies and undergo regular third-party security audits.

Has your system ever been compromised?

No, our system has never experienced any security breaches. Our voting platform's security record remains 100% intact. We take a proactive approach to security with **continuous monitoring** by Aikido Security and **routine penetration testing** by Websec Canada to identify and fix vulnerabilities before they become risks.

How is my vote protected from tampering?

Once you cast your vote, it is **encrypted and securely stored** in our electronic ballot box. The system ensures that no one—not even election officials—can alter or tamper with your ballot after it has been submitted.

Can anyone see how I voted?

No, your vote remains **completely confidential and anonymous**. While the system records that you have voted, it does not store or reveal who you voted for. Ballots are encrypted and anonymized, ensuring full privacy.

How do you prevent someone from voting multiple times or voting as someone else?

Our system prevents duplicate voting by **tracking all voting methods in real-time**. If a person votes online, the system immediately updates, ensuring they cannot cast another ballot in person or by mail. We also use **secure authentication methods**, such as personal information verification and one-time PINs for online voting.

Data Privacy & Protection

How do you protect against hacking attempts?

Our platform is designed with **multiple layers of security** to detect and prevent unauthorized access. We use real-time threat monitoring, routine security audits by Prescient Security, and the latest encryption standards to safeguard voter data.

How do you protect my personal information?

We take privacy seriously. All personal data is encrypted and stored securely, and we **never share voter information** with third parties. Our system follows strict privacy policies to keep your data safe.

Where is voting data stored?

All voting data is stored on **Canadian-based servers** in Montreal, Quebec, and Toronto, Ontario—ensuring compliance with Canadian privacy laws. As part of our commitment to **Indigenous data sovereignty**, OneFeather ensures that all data is managed in a way that respects Indigenous governance and control. Voting data is **encrypted both in transit and at rest** for maximum security, and we do not store any data outside of Canada.

Can my voting record be traced back to me personally?

No. Once a ballot is cast, it is **completely anonymized**, meaning it cannot be linked back to any individual voter.

What happens to my personal data after the election?

After an election, all personal data is **securely archived or deleted** according to strict privacy policies. No voter data is retained beyond what is legally required.

System Reliability & Backups

What happens if there's a temporary service interruption during voting?

Our system is built to handle unexpected issues, but if an outage ever happens, don’t worry—your vote is safe. We have **backup systems and recovery plans** in place to get everything back up and running quickly. Any votes already submitted are securely stored and won’t be lost. If there’s ever a disruption, election officials will be notified right away, and voters will be kept in the loop on what to do next.

How do you handle suspicious activity?

Suspicious activity triggers **automatic alerts** for investigation. Our security team works quickly to assess and address any risks.

How do you respond to significant system failures or security incidents?

Security is our top priority, and we have **advanced monitoring systems** in place to detect and prevent threats. If a security issue or system failure ever happened, we'd act fast using our **detailed response plan** to protect voter data and keep elections running smoothly. If needed, election officials and voters would be informed so they know exactly what's going on.

What backup measures are in place if online voting is compromised?

We have **redundant systems and secure backups** to ensure votes remain intact. If online voting were ever compromised, election officials would be notified, and alternative voting methods could be used.

Keeping Things Transparent

Has your system been reviewed by independent security experts?

Yes. Our platform undergoes **regular independent security audits** by Prescient Security and **penetration testing** by Websec Canada to ensure compliance with industry-leading security standards.

How do you stay current with evolving security threats?

We continuously **update our security measures** to stay ahead of emerging threats. Our team regularly assesses and improves protections to maintain a secure and trustworthy voting process. We follow OWASP (Open Web Application Security Project) guidelines and utilize Aikido security software, which provides real-time alerts about the latest threats and vulnerabilities in the cybersecurity landscape.

OneFeather

Still Have Questions? We've Got Answers!

voterhelp@onefeather.ca | support.onefeather.ca