

Pamphlet d'information sur la sécurité

Sécurité du vote en ligne pour Élections Yukon



Aperçu de la sécurité

Simple Vote Inc. fournira le système de vote par internet pour les Élections 2022 des Premières Nations et de la Commission Scolaire Francophone. Le système de Simple Vote est sécurisé et protège le secret de votre vote.

Bulletin de Vote Secret

Lorsque vous votez, votre bulletin de vote est instantanément encrypté et sauvegardé sans aucune possibilité qu'il soit relié à votre identité, tel qu'avec un scrutin papier traditionnel. Il est impossible pour le personnel électoral, les employés de Simple Vote, ou tout autre personne de voir le contenu de votre bulletin de vote. Les fonctionnaires électoraux ne pourront uniquement voir que vous avez voté, l'heure à laquelle vous avez voté et de quelle adresse IP le vote a été placé.

Une personne, un vote

Seuls les individus inscrits sur la liste d'électeurs seront autorisés à accéder au scrutin. Lorsque vous votez, votre nom est automatiquement ajouté à la liste de votes complétés et vous ne pouvez pas voter à nouveau. Même si vous essayez de voter en utilisant plusieurs appareils simultanément, le système n'acceptera toujours qu'un seul vote par électeur.

Vérification et Audits

Si nécessaire, Simple Vote fournit des auditeurs désignés avec les accès appropriés afin d'observer que le système permet de voter selon les règles appropriées, et empêche d'en faire autrement. L'Auditeur peut continuellement surveiller toute l'activité reliée au vote se déroulant avant, durant, et après la période de vote. Il est aussi impossible pour l'Auditeur de voir le contenu de votre vote.

Lorsque vous votez, un code de réception de vote est produit. Vous serez le seul à connaître ce code. Imprimez ce code ou prenez-le en note. Une fois la période de vote terminée, vous pourrez vérifier, à l'aide de votre code de réception, que votre vote a bel et bien été compté.

Protection contre les pirates informatiques

Simple Vote est un expert en sécurité internet et la plus grande importance est accordée à protéger le système de vote. Toutes les communications entre votre ordinateur et le site de vote sont encryptées pour assurer la confidentialité. Le bulletin de vote en ligne est inviolable et plusieurs couches de protection sont mises en place pour protéger les serveurs contre les attaques.

Protection Contre les Imposteurs

Pour voter en ligne, vous devrez entrer un mot de passe. Tous les mots de passe sont composés d'une valeur alphanumérique aléatoire qui sera envoyée par courriel à chaque électeur au début de la période de scrutin, dans une Lettre d'Information aux Électeurs. Comme mesure de sécurité supplémentaire, les électeurs devront entrer leur date de naissance pour compléter la procédure de vote. Par conséquent, si votre Lettre d'Information aux Électeurs se retrouvait entre de mauvaises mains, une autre personne ne pourra pas voter à votre place sans votre mot de passe et votre date de naissance.

Informations techniques

Sécurité optimale

Simple Vote a été intégralement conçu pour minimiser le risque de fraude électorale ou de violation du secret :

- ✧ Les électeurs qui tentent de contourner l'authentification ou ont déjà voté se voient refuser l'accès au bulletin de vote.
- ✧ Nous garantissons « un vote par électeur » en marquant les électeurs comme ayant voté et en enregistrant le vote en une seule et même transaction. Même si un électeur soumet le bulletin de vote simultanément sur plusieurs appareils, cette technologie garantit qu'un seul vote est accepté.
- ✧ Les bulletins de vote sont rigoureusement vérifiés avant d'être acceptés.
- ✧ Toutes les activités des administrateurs et des électeurs sont enregistrées avec horodatage et adresse IP.
- ✧ La communication entre l'ordinateur de l'électeur et notre site Web est cryptée avec *TLS 1.2* et des suites de chiffrement robustes pour protéger contre les attaques de cryptage actuelles et futures.
- ✧ L'ensemble de la base de données du système de vote est chiffré au repos à l'aide du chiffrement *AES-256*.
- ✧ Nos serveurs sont « renforcés » et soumis quotidiennement à des scans de sécurité conformes à la norme *PCI Trust Guard*.
- ✧ Notre système de vote est régulièrement soumis à des tests de pénétration par *CyberHunter* et à des audits de sécurité du code source par *HP Fortify*.
- ✧ Simple Vote adhère aux directives établies par l'*Open Web Application Security Project*.
- ✧ Tout changement apporté au système de vote doit faire l'objet d'un examen de sécurité interne avant d'être mis en ligne.
- ✧ Tous les postes de travail du personnel sont tenus à jour et protégés par un mot de passe d'accès, un pare-feu, un antivirus, un anti-spamware et un cryptage de disque.
- ✧ Tous nos courriels sont authentifiés avec le protocole *DMARC* afin de protéger les électeurs contre l'hameçonnage.
- ✧ Nos serveurs sont protégés par un pare-feu très puissant, *FortiGate Unified Threat Management*, qui comprend un *système de détection des intrusions* et un pare-feu redondant de secours immédiat.
- ✧ L'accès au réseau est protégé par un réseau privé virtuel (VPN) et l'authentification à deux facteurs (A2F).
- ✧ Simple Vote emploie une solution automatisée conçue par *Radware* pour se protéger en continu contre les attaques par déni de service (DoS).
- ✧ Nous sommes protégés contre les attaques DoS au niveau DNS grâce à notre infrastructure Anycast.

Fiable et entièrement hébergé

Simple Vote est un logiciel-service (SaaS) en infonuagique bâti sur du matériel IBM haute-performance, avec une redondance complète sur l'ensemble de l'infrastructure (pas de points de défaillance uniques). Notre centre de données se trouve dans une zone montagneuse stable, à l'abri des tremblements de terre, des ouragans, des tornades et des zones de climat violent. Le centre de données contient une infrastructure d'alimentation, de refroidissement et de sécurité avancée, ainsi qu'une architecture réseau Cisco Data Center 3.0. Il est doté d'un personnel 24 heures sur 24, 7 jours sur 7, soutenu par un centre d'opérations réseau hors site. Nous utilisons également plusieurs clusters DNS Anycast pour garantir la tolérance aux pannes au niveau DNS.

Simple Vote utilise des outils de surveillance externes pour surveiller automatiquement les principaux « signes vitaux » de notre système de vote 24x7 et un membre du personnel technique est immédiatement informé de toute anomalie. Simple Vote possède un plan de reprise après sinistre ainsi qu'un site dynamique dans un centre de données de sauvegarde situé dans une zone géographique différente. Le site dynamique est synchronisé avec le centre de données principal à l'aide de la réplication de base de données à distance. Si le centre de données principal connaît une panne, nous avons la possibilité de rediriger rapidement le trafic de l'ensemble du système de vote vers le site dynamique, en minimisant les perturbations aux scrutins en cours et en évitant toute perte de données. Vous pouvez être assuré que votre scrutin est toujours protégé et disponible en cas de catastrophe.

Confidentialité

Simple Vote prend très au sérieux le secret du vote. Il est impossible pour les organisateurs de scrutins de déterminer ce qu'un électeur a voté puisque les résultats sont anonymes. Toutes les informations de l'électeur sont supprimées de nos serveurs si vous choisissez de supprimer le scrutin. Nous n'utilisons jamais l'information de l'électeur pour autre chose que le vote et ne partageons jamais ces informations avec des tiers. Notre politique de confidentialité (disponible sur le site Web de Simple Vote) et notre système de vote ont été certifiés de manière indépendante par TRUSTe pour la conformité à leurs exigences de certification de la confidentialité et de Trusted Cloud.



McAfee Enterprise-Ready Rating

Simple Vote a reçu la note CloudTrust la plus élevée de McAfee. McAfee effectue des évaluations objectives et approfondies des services infonuagiques basés sur un ensemble détaillé de critères développés en collaboration avec Cloud Security Alliance (CSA). Les services désignés McAfee Enterprise-Ready répondent pleinement aux exigences les plus strictes en matière de protection des données, de vérification d'identité, de sécurité des services, de pratiques commerciales et de protection juridique.



Conformité SOC 2



Simple Vote est conforme à la norme SOC 2 Type 1. Le SOC 2 est une norme d'audit largement reconnue et publiée par l'American Institute of Certified Public Accountants (AICPA). Un rapport d'audit détaille la capacité d'un fournisseur de services à offrir des contrôles et des garanties adéquats lorsqu'il héberge ou traite des données appartenant à ses clients. L'audit se concentre fortement sur les domaines de la sécurité, de la disponibilité et de la confidentialité. Il aborde des sujets importants tels que la sauvegarde et la restauration, les opérations informatiques et les ressources humaines.

Les centres de données où se trouvent les serveurs de Simple Vote sont également conformes à la norme SOC 2 Type 2. Cette attestation est une validation indépendante de la qualité, de l'intégrité et de la fiabilité de l'infrastructure et des services de Simple Vote.



Protection avancée contre les attaques DDoS

Avec Radware

Les attaques par déni de service (DoS pour Denial of Service en anglais) sont plus fréquentes et ont évolué pour devenir des défis complexes et accablants pour les petites et grandes organisations. Même si les attaques DoS ne sont pas un phénomène récent, les méthodes et ressources disponibles pour conduire et masquer ces attaques ont dramatiquement évolué pour inclure des attaques distribuées (DDoS) et, plus récemment, distribuées réfléchies (DRDoS).

Les services de protection contre les attaques DDoS de Radware surveillent tout le trafic entrant sur le réseau pour prévenir les attaques flood de gros volume qui visent à perturber les services. Cette protection est l'une des meilleures et inclut la détection basée sur le comportement en utilisant des algorithmes avancés et brevetés d'apprentissage automatique, protégeant contre les menaces connues et inconnues, la protection contre les attaques DDoS de niveau réseau et/ou de couche d'application, la protection contre les attaques flood cryptées sans nécessiter des clés de décryption et sans ajouter de latence en temps normal, ainsi que de nombreuses options de conformité et de certifications, au-delà de leurs rivaux, et incluant des certifications spécifiques à l'industrie tels que PCI et HIPAA, des standards de sécurité infonuagique tels que SOC 2 Type II, ISO 27001, ISO 27017, ISO 27018, ISO 27032, etc.

Simple Vote jouit de la protection d'une solution active en permanence qui combine les appareils de mitigation d'attaques Radware DefensePro avec leur service de protection DDoS infonuagique. Le système DefensePro filtre localement tout le trafic entrant dans l'infrastructure infonuagique privée de Simple Vote, située aux centres de données TeraGo. Si de la capacité de mitigation supplémentaire est nécessaire, le système DefensePro déclenche automatiquement une redirection du trafic vers les centres de scrubbing infonuagiques de Radware. Cette solution hybride permet un équilibre entre la protection en temps réel et latence minimale d'une solution sur place, et d'autre part avec la capacité massive d'un service infonuagique qui est activé sur demande.

Les centres de données



Sécuritaire et fiable

- Authentification multi-facteurs avec surveillance et supervision
- Infrastructure électrique et mécanique ultra redondante
- Surveillance 24/7 par deux Centres des Opérations Réseau Canadiens géo-redondants

Normes des meilleures pratiques

- Conforme aux normes de gouvernance
- Suit la méthodologie ITIL de gestion de services avec du personnel certifié
- Infrastructure redondante et surveillance 24/7

Recouvrement après-sinistre d'entreprise

- Données situées au Canada
- Plusieurs options de location pour des sites secondaires géo-redondants
- Capacité flexible

Installations

TeraGo possède et opère cinq centres de données au Canada. Voici des détails additionnels sur leurs centres de données dernier cri à Kelowna, Colombie Britannique, et Mississauga, Ontario, utilisés par Simple Vote.

Category	Kelowna, BC	Mississauga, ON
<i>Designed to DC Tier</i>	Tier III	Tier III
<i>Power Redundancy</i>	2N	2N + 1
<i>Max Power Density</i>	Up to 5 kVa	Up to 18 kVa
<i>Backup Generator Capacity</i>	> 48 hours at full load – across all facilities	
<i>DC Network Connectivity</i>	10 Gbps +	10 Gbps +
<i>Carrier Redundancy</i>	Multiple Tier 1 providers	Multiple Tier 1 providers
<i>TeraGo Hybrid Cloud Capable</i>	Yes	Yes
<i>Compliance</i>	AT101 SOC Type II and SSAE 16 – across all facilities	
<i>Security</i>	24/7 security and video monitoring, multi-factor biometric access authentication, man traps, proximity scanners	
<i>Support</i>	24x7x365 support	



Kelowna, BC:

- Placé stratégiquement dans une des régions les moins à risque de l'Amérique du Nord
- Design « Gigavault » unique, des boîtiers à murs solides qui fournissent des espaces clos et séparés
- Installations neutres des opérateurs avec diverses connexions de plusieurs fournisseurs
- Installations au design efficace et vert munies d'allées froides fermées et du refroidissement à l'air durant l'hiver
- Design conforme aux normes du « Uptime Institute Tier III », qui inclut l'infrastructure énergétique redondante 2N+1 de sous-stations en anneau

Mississauga, ON:

- Installations de dernier cri dans la région du grand Toronto
- Plus de 1 MW de capacité énergétique critique totale
- Installations neutres des opérateurs avec diverses connexions et une connexion directe à 151 Front
- Design conforme aux normes du « Uptime Institute Tier III », qui inclut une connexion à deux sous-stations pour les services et une architecture énergétique 2N

Pour plus d'informations, veuillez écrire à info@simplyvoting.com