EVOTE

everyone counts®

Evote has been delivering secure, reliable, cost-effective online voting since 2003. We work together with Everyone Counts, the respected global leader in electronic election solutions, established in 1997, combining unmatched election technology and expertise, hardened solutions, professional services and highly skilled and experienced staff. Everyone Counts has enabled millions of voters in over 160 countries to participate in local, regional and national elections with an accessible, secret ballot, securely delivered via the internet or by telephone.

Clients include governments, political parties, corporations, financial institutions, unions, universities, associations and myriad other entities including KPMG, Ernst & Young, Deloitte and PriceWaterhouseCoopers accounting firms. Our expertise is technology and election experience.

We believe that every eligible voter, regardless of geography or any accessibility issues, should have the opportunity to exercise the right to the vote. You can trust us to deliver the right solutions for your election challenges.

Data Security
We use state of the art SAS 70 Type II, TIA-942 Tier 4 data centres with multiple internet connection providers, configured for automatic failover. All hardware is stored within a secure facility and security protocols ensure only trusted personnel have access to election servers, with man-trapped security and key card and biometric access validation. All election servers are encased within steel cages in a secured area, with access controlled and monitored on-site 24/365. We use redundant, normalized power systems to ensure steady clean power and all data centres are strategically selected for ability to utilize two power grids for an extra layer of redundancy. Each data centre is climate controlled and has diesel generators independent of external power.

Systems Security
Securing and maintaining the hardware and software on which the election is run and data is stored is paramount to establish confidence in the results of an election. We have multiple redundancies and highly available load balancers to ensure and evenly distribute load across multiple election servers. Our software is designed to prevent and detect any intrusion coupled with controlled access to all election hardware and software to help ensure the security of election content and any stored data. Redundancies are built into the architecture of each election by way of a shared-nothing, no single-point-of-failure design to minimize any failure and all systems are protected by enterprise grade firewalls and intrusion detection systems to enforce our strict rules associated with each election server. All unauthorized activities are proactively blocked, logged and reported for investigation. Our election servers run the latest version of CentOS Linux with all available security patches and all software packages installed on election servers are monitored and maintained at the latest available, secure and stable version.

Ballot Transmission
All information transmitted between the voter's browser and the election server is encrypted utilizing Secure Socket Layer (SSL) transmission that employs AES 256-bit encryption with 2048-bit keys. The SSL protocol enables voters to securely communicate in a way that is designed to prevent and detect eavesdropping, tampering or communications forgery. SSL is the same protocol used by banks and e-commerce companies to keep your information secure in transactions, and similarly keeps voter communications private within our hardened systems and processes.