

Why did you select BigPulse?

BigPulse operates at the leading edge of democracy technology. The company cultivates a meticulous attitude toward all aspects of security and risk management. BigPulse has pioneered numerous vote security innovations and specialises in high security online elections. With approximately 1,000 clients in 35 countries, BigPulse's technology supports 17 different languages and they excel in complex, high-security elections. BigPulse is independent. The company and key people involved have no political affiliations or interests that could compromise the independence or integrity of its activities. BigPulse has reported to have run over 90,000 secure polling events in 30,000 polling groups and has harvested more than 12 million online votes.

No organisations support or use electronic voting.

That's not true according to BigPulse. Their clients include leading universities, small and large companies, trade associations, peak body industry and professional groups, law firms, chambers of commerce, publishers, unions, clubs, NGOs, market researchers and hundreds of schools in education projects.

So if the NZPFU needs support, this support now has to come from the USA?

No, BigPulse has an office based in Australia. They also offer 24-hour support. During the trial electronic vote, we were supported by staff in Australia (outside of NZ business hours and over weekends).

Won't this system be expensive if we have to pay for every ballot we run?

BigPulse offer a subscription model where we can run as many ballots as required for a single fixed price, fully supported. The term can be for 3, 6 or 12-months at a time.

Will this end up saving the NZPFU time, money and effort?

We think so. We'll be able to run high security online elections and avoid all the cost, effort and expense of printing, posting and counting paper ballots. Members can vote online from anywhere and the result is known immediately after vote close.

Is their system secure?

Yes, BigPulse is meticulous about all aspects of security and risk management. Security is much more than 256 bit TLS/SSL encryption, it covers things such as voter authentication, data protection, vote integrity, secure anonymous voting, server reliability and access control.

But, is this really a secret vote?

The BigPulse database records your vote in a manner that is de-linked from your personal data. This means it is de-linked from the voting account you used to submit the vote. Your voting account will retain the time you submitted the vote, your IP address and browser signature. There is no link in the database, either direct or indirect, between your voting account and the choices you selected when submitting the vote. Your vote is immediately de-linked from your voting account as soon as it is recorded in the database. No copy of the vote receipt sent is retained. We call this absolute anonymous vote storage because no one, not even BigPulse engineers, can determine how you voted by viewing the database records.

If we adopt electronic voting, we will find that voter turnout will decrease.

The Auckland Local Triennial Election proved otherwise. First, a paper vote achieved a 77% return. The electronic election then achieved a 89% turnout. This represents a 16% increase. BigPulse report that clients frequently experience a 50 to 100 per cent increase in voter turnout. Voters respond to the convenience of online voting, ease of use and vote reminders sent to people who have not voted.

Can the NZPFU watch as the votes are counted live and then influence members who have not yet voted?

No, poll administrators cannot view the live counts in the online ballots. Vote counts remain suppressed until after vote close.

Why were some candidate biographies missing from the online ballot form?

Those candidates chose not to provide biographies.

What if I am on leave when voting opens?

The trial election by electronic voting was purposely scheduled to fall over different leave groups to capture any member on annual leave.

What if I'm overseas or sick?

During the trial electronic vote, for members who could not access their voting link we sent a new secure link to the members personal email account.

What if I vote using the link sent to my personal address and then login to the FENZ portal and vote again using that link?

This is not possible – the platform automatically prevents duplicate voting.

What if I don't receive the secure link in my email at all?

We can easily resend a secure voting link to you.

What if the email you send bounces?

We monitor for any bounced emails.

Why was the secure voting link sent to my FENZ email?

Every fortnight FENZ provide the Union with a database of current financial members. This is the most accurate and secure way we can identify current financial members as our membership changes from pay period to pay period.

Will the NZPFU know how I voted?

No, the database records your vote in a manner that is de-linked from your personal data. In fact, we did not even provide a single members name to BigPulse.

The NZPFU may not know who I voted for but if I vote using the FENZ network, my Employer will know how I voted.

No, this is not correct. A valid 256 bit TLS/SSL (Secure Sockets Layer) Certificate secures the BigPulse platform. This security protocol secures and encrypts communication between your web browser and

the BigPulse platform. SSL encrypts the information members send to, or receive from, the electronic voting platform. This keeps any undesirables from spying on any exchange between BigPulse and our members. This is the industry standard for web security and means that the information members enter on the voting platform is private and can't be viewed by a third party.

But is 256-bit encryption enough?

We think it's more than enough. To crack a 256-bit encryption key by brute-force, there would be 256 possible combinations – a hacker would need to try most of the 2^{256} possible combinations before arriving at any conclusion. On paper, 2^{256} may seem like just a number, but don't underestimate its power. 256-bit will have

15,792,089,237,316,195,423,570,985,008,687,907,853,269,984,665,640,564,039,457,584,007,913,129,639,936 (78 digits) possible combinations. No Super Computer on the face of this earth can crack this. DigiCert estimate that standard desktop computing power would take 4,294,967,296 x 1.5 million years to break a 2048-bit SSL certificate. Or, in other words, a little over 6.4 quadrillion years.

FENZ bosses have the ability to read every email sent through their network.

True. But this system does not use email to transmit a members vote. Your vote is sent securely and is encrypted.

Is the system transparent though?

The transparent vote verification process allows all voters to self-audit the vote counts and verify the accurate recording of their own votes with ease. It's a level of security and transparency that's impossible with old style paper voting.

Can you provide a means for voters to confirm the full list of all candidates and candidate presentation order as it appeared in the voter's ballot?

Yes.

The fundamental flaw with electronic voting is that voting must be able to be verified. That is, there must be a record where any voter can verify their selection against the count for a transparent audit.

BigPulse enables the vote count integrity of a secret voting election or referendum to be verified without reference to the black-box servers used to harvest the votes. Members can be issued with full take-home receipts. We can then provide receipt owners with ready access to the full list of vote receipts with all personally identifiable information removed from each vote receipt.

Can you issue tamper proof vote receipts?

Yes.

Can you offer a secure method for transferring vote receipts to voters?

Yes.

What if I forget to vote?

We will continue to send reminder emails up to the close date to those people who have not yet voted.

What if I vote after the close date?

We set the vote open and close date and time in our time zone. The voting will open and close automatically at these times – it's not possible to vote after the vote close time.

Can I vote from a mobile device?

Yes! Our platform is mobile friendly. In fact, over 12% of votes were made from mobile devices during our trial election.

So now my email address and voting account data is being kept and stored in the USA?

No, within about six weeks, but not before one month, BigPulse will delete all voting accounts. Votes are not deleted unless requested because they do not contain personally identifiable data and can remain as a useful historical record. Ballot details are retained and provide useful templates for further elections.