Eleven essential principles for an Australian internet voting service

The following eleven essential principles for an internet voting service were endorsed by the Electoral Council of Australia and New Zealand (ECANZ) on 4 July 2017.

In developing these principles, the ECANZ examined the United States Election Assistance Commission's 'Voluntary Voting System Guidelines (VVSG 2.0)', and the Council of Europe's intergovernmental standards for e-voting (CM/Rec (2017)5) - drawing on these standards and principles to develop eleven essential principles to guide the design and implementation of an internet voting service in Australia for use by all member Electoral Commissions.

Enfranchisement

Accessibility

– as far as is practical, all eligible people should be able to access the internet voting service

The internet voting service shall be designed, as far as practicable, to enable eligible voters to vote independently regardless of disabilities, technology or geography. The internet voting service will be an additional and optional service for specific eligible voters to use. It would be offered in conjunction with other pre-existing methods of voting.

Usability

– the process of internet voting should be sufficiently easy for eligible people to cast a vote

The user interface of the internet voting service should be easy to understand, intuitive, and able to be used by all eligible voters on multiple technology platforms. Information provided may be presented differently depending on the differing technologies and channels which the service can be accessed on. For example, the electoral content presented on an electronic ballot paper will be the same as on the physical paper ballot paper (ensuring impartiality and equitably); however changes may be made in accordance with relevant legislative provisions while ensuring usability on each technology platform.

One person, one vote

– the ability to ensure that each eligible elector receives only their voting entitlement

The internet voting service should enable each eligible voter to be uniquely identified, ensuring that they are distinguishable from other voters. The service should cater for any legislative requirements around the presentation of identification documents. An eligible voter will only be able to use this channel if they can be uniquely identified this way. The service will check eligibility and only grant access to those that have been authenticated as an eligible voter. The service will have a process to ensure that only one vote per eligible voter is admitted to the count.

Integrity

Security

– prevention of loss, corruption or tampering of votes

The internet voting service and responsible Electoral Management Body shall protect authentication data so that unauthorised parties cannot misuse, intercept, modify, or otherwise gain knowledge of this data. The authenticity, availability and integrity of the electoral roll and lists of candidates shall be maintained. Only persons authorised by the electoral management body shall have access to the central infrastructure, the servers and the electoral event data.

The audit system should be able to detect voter fraud and provide proof that all counted votes are authentic. The audit system shall be open and comprehensive, and actively report on potential issues and threats. Where incidents that could threaten the integrity of the service occur, those responsible for operating the equipment shall immediately inform the electoral management body. Procedures shall be established to ensure regular installation of updated versions and corrections of all relevant software as the service will need to be continually evolved to meet and protect against potential and actual issues and threats.

The service will encrypt votes if they are to be stored or communicated outside controlled environments. The electoral management body shall handle all cryptographic material securely. Votes shall be kept sealed[1] until after the close of polling.

Robustness

– the system and processes are not subject to significant interruption or failure

Robustness applies to people, process and technology. The internet voting service must be available, reliable and secure to ensure that it can function on its own, irrespective of shortcomings in the hardware or software. The technical solution for the service will be peer-reviewed to help ensure availability, reliability, usability and security. The service shall identify votes that are affected by an irregularity so that necessary measures are taken and stakeholders are informed. The electoral management body administering the service will ultimately be responsible for respect and compliance with the above even in the case of failure.

Transparency

– the service and processes be designed to enable scrutiny, to provide stakeholder confidence

The internet voting service and accompanying processes will be established with a focus on transparency. The service will ensure that the way in which eligible voters are guided through the internet voting process shall not lead them to vote without due diligence or without confirmation. The service should be designed to allow the voter to express his or her true will. A voter will be allowed sufficient time to consider their choices and will be under no obligation to commit their vote without time for reflection on their choices. Upon casting their vote, the service will verify to the voter that his or her intention is accurately represented and that the vote has been submitted. Any alteration to the voter's vote should be detected by the service.

---

[1] Sealed is an analogy to the seal on a physical ballot box. This is the term used in the European standards

Voters and third parties should be able to observe the count of the votes and check that only eligible voters' votes are included in the results. The service will provide evidence that only eligible voters' votes have been included and this evidence will be auditable.

Clear and unambiguous information about the internet voting service should be available to the public explaining how to use the service and how the service operates.

The service should be open for verification, assurance and scrutiny purposes. Observers, to the extent permitted by law, shall be enabled to observe, comment on and scrutinise the internet voting component of an election, including the compilation of the results.

Independence

– full control of the system and processes shall rest with the Electoral Management Body

The electoral management body will be accountable for the internet voting service of an electoral event. The Council can ensure that the capability to run an event is available to each electoral management body outside of external providers. The relevant legislation shall regulate the responsibilities for the functioning of the service and ensure that the electoral management body has control over them.

Impartiality

– the voters intention should not be affected by the voting service

An eligible voter's intent should not be affected by the internet voting service. The service will ensure that the way in which voters are guided through the process and the information displayed will not influence their vote.

The service should be structured to ensure that voter's do not miss anything during the voting process. It should provide a means for informal voting by allowing a blank vote to be cast, however advising the voter they would be casting an informal vote and providing them with the option to change their vote if they wish. This provides an equitable approach across channels enabling voters to cast an informal vote via both the service and the paper-based option. Other than a blank ballot paper, all formality rules will be enforced by the service.

Accuracy

– the service should accurately capture, store and export the voters intention

The internet voting service shall provide sound evidence that only votes from eligible voters are included in the final result while de-identifying a completed ballot paper from its voter. The service shall support the voter in marking the ballot paper and accurately store, capture, verify, and export the vote cast. Before an event, the electoral management body administering the service shall satisfy itself that the service is genuine and operates correctly.

The service shall allow and support evaluation regarding the compliance of the service and its related components. This should occur upon introduction, periodically and after significant change to the service has been made.

Privacy

Privacy of personal information

- the system and processes shall maintain the privacy of personal information

The internet voting service shall process and store, as long as necessary, only the personal data needed for the conduct of the electoral event. The electoral management body administering the service will determine what information is deemed necessary to keep and dispose in accordance with relevant legislative obligations. Any information retained will be secure and any unnecessary information will be disposed of.

Secrecy of vote cast

– the service shall maintain the secrecy of the votes cast

The internet voting service shall be organised in such a way as to ensure that the secrecy of the vote is respected at all stages of the voting process – from pre-polling through to counting of the votes. Votes shall remain sealed until the counting process commences. During completion of the ballot paper, the service will protect the secrecy of the voter's choice. The service shall not assist the voter with proof of the content of the vote submitted for use by third parties.

The service will be able to de-identify a voter from their completed ballot paper to preserve the secrecy of the ballot. The order in which votes are cast shall be mixed as to deny reconstruction of the order of votes submitted.