



NATIONAL
DEMOCRATIC
INSTITUTE

Recommendations for the Adoption of Electronic Electoral Technologies

2022

Table of Contents

Introduction	1
Recommendations for all election stakeholders	1
Inclusion	2
Secrecy	2
Integrity	2
Universality	3
Equality	3
Transparency	4
Accountability	4
Security	5
Public confidence	5
Electoral authorities	5
Prior to the election process	5
During the election process	6
Post-election	7
Parliaments	7
Electoral dispute resolution bodies	8
Specialized national agencies	8
Political parties and candidates	9
Civil society	9
Vendors	10
International donors and technical assistance providers	11
Conclusion	12

Introduction

As electronic electoral technologies (EETs) are increasingly introduced to automate aspects of the election process, there is a growing awareness of the need to ensure that key human rights election principles are respected. The following recommendations accompany the paper *General Principles and Guidelines Related to Information and Communication Technologies (ICT) and Elections*, which was drafted by a number of endorsing organizations of the Declaration of Principles for International Election Observation (DoP).

Based on the guidelines, the recommendations are divided in two parts. The first part highlights actions that all election stakeholders need to take to ensure that key election principles relevant to the implementation of EETs are respected. These key election principles include: inclusion, secrecy, integrity, universality, equality, transparency, security and public confidence. The second part includes recommendations aimed to ensure that each stakeholder meets its responsibilities to ensure the integrity of the election process. These include specific recommendations for the election management body (EMB), parliament, national agencies, political parties, judiciary, civil society, vendors of election technologies and international donors.

The implementation of EETs involves a number of stages, and could take a significant amount of time. This document includes recommendations for the various stages for the consideration, introduction and use of EETs in the election process. Electronic technology tools may automate a number of election processes, such as voter registration (increasingly with biometric voter registration systems), voting, counting and results tabulation. The recommendations contained in this document generally apply to the introduction of EETs for any aspect of the election process.

These recommendations aim to provide a useful basis for considering how EETs can be implemented in a way that is consistent with international human rights commitments for election integrity. As international election observation missions (EOMs) and citizen observers increasingly monitor elections that incorporate new technologies, these recommendations may also serve as a model for those who are assessing election processes and recommending improvements in line with international and regional human rights commitments.

Recommendations for all election stakeholders

All actors involved in an electoral process, including EMBs, political parties and candidates, government institutions, civil society and private companies supplying goods and services, have a responsibility to ensure the integrity of the process. Similarly, all stakeholders have a responsibility to make sure that the adoption of EETs contributes to more transparent, inclusive and accountable processes. Towards that goal, all election stakeholders should ensure that any EET system adopted for election processes respects key election principles guaranteed by international and regional human rights instruments. These include: inclusion, secrecy, integrity, universality, equality, transparency, accountability, security and public confidence.

Inclusion

The introduction and implementation of EET systems should take an inclusive approach, involving a broad range of stakeholders throughout the process, to promote transparency and public confidence.

- Allow adequate time and funding for the proper deliberation and implementation of any EETs in line with international good practice. Time needs to be allowed for the public consultation, needs assessment, feasibility study, procurement, legislative changes, piloting, certification and testing processes to be carried out, and parliamentary oversight, and legal accountability. This often requires more than one election cycle.
- Provide for a broad consultative process that is inclusive of political and civil society actors, to discuss specific problems to be addressed, and potential EET tools to address them. This process should take into account the widest possible spectrum of opinions to build political consensus, public confidence, and ensure that universal and equal suffrage are not compromised by adopting EETs.

Secrecy

EET systems must be consistent with the principle of secrecy of the vote.

- EET systems must not allow identification of a specific voter's choice and voters must not be able to prove to anyone how they voted.
- Any electronic voting technology that verifies the voter's identity must not have any link between that record and the voter's choice.
- Any record of the order in which voters cast their votes could be used to identify how they voted, and thus also violates voter secrecy and must not be permitted by the system.
- Due to security and vote secrecy concerns, at this time internet voting is not advisable. Such systems, if used, must ensure that the voter's identity is not linked to the vote.

Integrity

EET systems must ensure the accuracy and security of each step in the electoral process, in line with the electoral framework.

- For voting and counting systems, votes must be cast as intended and recorded as cast. Voters should be provided with the means to verify this, including a voter verified auditable paper trail (VVPAT).
- Integrated software that both captures and counts voters' choices increases the risk that a citizen's ballot will not be counted as cast, either through software errors or malicious programming. To reduce this risk, EETs used to prepare ballots (i.e. ballot-marking devices) should be separate from EETs used to count and tabulate ballots (scanners).

- Results tabulation systems must ensure that the transmission and tabulation processes are secure and cannot be altered by undetected fraud or error. Results must be immediately and publicly available at polling stations and at each level in the tabulation process to allow timely independent verification by electoral contestants, civil society actors and other stakeholders. Results at each level should be immediately available in a machine-readable format on the Internet and preserved to facilitate such verifications.
- Voting and counting systems must allow for timely and meaningful verification through processes such as manual recounts, end-to-end verifiability and/or post-election audits. For this to be possible, voting systems must provide a paper record such as a VVPAT.
- Voter registration systems should also guarantee the accuracy of voter records. The accuracy of the voter register can be assessed through audits conducted by the EMB or its independent consultants, or through independent verifications conducted by civil society organizations.
- Paper-based back-up solutions should be available in the event that EETs, including electronic voter lists, voting machines and results tabulation systems, fail on election day.

Universality

The use of technology in the election process must not discriminate against any group of voters or discourage them from participating. If the adoption of particular technologies would give advantages to certain segments of the population, thereby diminishing universal suffrage, that technology should not be adopted.

- Electronic or biometric voter registration systems should be fully inclusive. Special efforts may be necessary to facilitate the registration of women, older people, persons with disabilities, religious or language minorities, or other traditionally marginalised groups.
- EET systems should not be the exclusive method of voting so as not to discourage less computer-literate persons from voting. For such cases, paper balloting should be available.
- Any EET should be designed to maximize universal accessibility of electoral processes for all groups, such as persons with disabilities, illiterate voters and those from linguistic minorities.

Equality

The use of EETs should ensure that no voter is permitted to vote more than once, safeguards are provided to prevent unintentionally “under” or “over” voting, and voters have an equal opportunity to use EETs in voter registration and voting.

- Where biometric voter registration has been implemented, the system should provide the possibility for de-duplication to avoid multiple registrations.

- Where EETs are used for voting alongside paper ballots, all means of voting should be equally available to voters. The availability of equipment and voting materials must be equally available to all communities.
- EETs must include safeguards to prevent voters from casting more votes than is established by law and from unintentionally omitting to vote for some offices or referenda, and must also ensure that no valid votes are subtracted from the system.
- EET voting systems should be able to prevent voters from casting an invalid vote. However, these systems should provide voters with an option to cast a blank ballot to allow them to participate in the process if they are dissatisfied with the available ballot choices.

Transparency

To enhance stakeholders' trust in EETs, every step of the process should be open to meaningful scrutiny by electoral actors (political parties, election observers, media, courts and voters).

- Citizen election observer groups and political contestants should be permitted to oversee all stages of the adoption of EETs, including access to relevant documentation on processes such as procurement, piloting and certification.
- Copies of the preliminary electronic and biometric voter registers should be made available to political contestants and citizen observers so that they can assess their accuracy. Data protection requirements and privacy safeguards should be respected in that process.

Accountability

While EMBs are the main focus of accountability in the electoral process, including with the implementation of EET systems, other stakeholders such as vendors, certification bodies and others involved in their procurement, management and use must also be accountable to the public for their actions, including through administrative sanctions and civil and criminal penalties.

- The use of EETs must be accompanied by verifiable mechanisms that record each action taken in the system.
- The EMB should ensure that it has ownership over all aspects of the EET system, including the collection and storage of data that is subject to the country's legal jurisdiction and requirements. The role of EET vendors must be clearly defined so that the EMB remains in control of the process at all times. The EMB must ensure that the process meets all deadlines and legal requirements and should oversee vendors. The legal framework should include appropriate measures to ensure these criteria are met.
- Election dispute resolution bodies such as the judiciary should be provided with the necessary technical expertise to adjudicate complaints that involve the use of EETs.
- Legal frameworks concerning the acquisition and implementation of EETs must clearly define administrative and criminal sanctions for actions that violate the law.

Security

Given potential vulnerabilities of EETs to interference from both domestic and foreign malign actors, there is increased awareness of the need to prioritize cybersecurity measures. Such vigilance helps to promote public confidence in the integrity of EETs.

- The use of EETs should comply with the international principles of data protection and privacy as well as any requirements of domestic and international law.
- Voter registration systems should ensure that the personal data of voters is securely stored and that it is used only for the purposes prescribed by law, while also meeting requirements for transparency to ensure verifiability of their integrity and requirements for equality and universality.
- Robust cybersecurity mechanisms must be developed to protect the integrity of election infrastructure, including systems that detect any efforts to probe, tamper with, or interfere with EETs.
- Consider conducting regular “adversarial testing”¹ to ensure the security of the systems against potential threats.

Public confidence

Lack of public trust can be a significant obstacle to the implementation of EETs. To overcome this, EMBs and other stakeholders should take measures to enhance public confidence in the use of EETs through inclusive consultation, transparency mechanisms such as citizen election observation, and public information at each stage of the process.

Electoral authorities

The EMB has primary responsibility in designing and implementing electoral processes that garner the trust of citizens and electoral actors, and fully reflect the will of the people. They have primary responsibility to ensure that any new EET contributes to the election process without introducing instability or barriers to the participation of citizens or electoral stakeholders.

Prior to the election process

- Conduct a feasibility study as the basis for the deliberation on the adoption of the EET. The study should consider the specific country context, the needs that are to be met by EETs, whether potential solutions are technically feasible and can meet the identified needs, anticipated benefits and potential risks of different options and the possible implications of any options, including financial and legal implications.
- Define technical specifications of the EET solutions that the country has decided to adopt, including by specifying the key election principles that must be safeguarded by EET vendors.

¹ Adversarial testing is a process in which ICT specialists attempt to identify security weaknesses or other flaws in the system in an unscripted manner.

Specialised government agencies (such as cybersecurity and data protection agencies) may need to be involved at this stage to assist, in addition to possible external expert support from technical assistance providers.

- Oversee the tendering and procurement for EET solutions acting in line with the national public procurement and anti-corruption frameworks (which should be based on transparency, competition and objective criteria in decision-making). Non-competitive processes or rushed tenders awarded under non-transparent conditions should be avoided, as these may have negative implications such as solutions that do not work as intended, potentially compromising the integrity of the election process.
- Throughout the introduction of EETs, take steps to ensure that the national electoral authorities retain full ownership and control over all aspects of the electoral process. While vendors may provide technicians to the EMB to support the EET system, they should not in any way replace functions of the EMB. The EMB may need to hire ICT staff with particular skill sets or launch capacity building programmes to ensure the necessary in-house expertise is in place to administer elections with the selected EETs.
- Ensure that the necessary legal framework (legal provisions and regulations) is in place to introduce EETs in elections. EMBs and parliaments must work together and include political parties, civil society actors and other stakeholders to support drafting of any necessary amendments or legislation.
- Conduct piloting of any identified EET solution in a small-scale election, such as a by-election or part of a municipal election with lower stakes, before introducing an EET in a nationwide election. Such a piloting exercise would provide valuable information on the reliability of the solution and its appropriateness for the context, as well as lessons learned that can be considered for a nationwide launch. Public education should also be conducted about the pilots for citizens directly involved and across society to build public confidence as the use of proven technologies is expanded.
- Carry out certification processes of the selected EET system in line with the standards and requirements of the national legal framework, making documentation of the process available to stakeholders. Such standards should include strong cybersecurity requirements.

During the election process

- Provide adequate training for election officials at all levels on the functioning of EETs and what specific steps to take in case of any malfunctioning.
- Conduct comprehensive voter education initiatives explaining new EETs to voters so that they have trust in the system and are prepared to use it during the election process. This must include information on the transparency and verification measures employed in adopting all sensitive systems such as voter registration, voting, and results transmission, tabulation and announcement.

- Provide testing of all EET equipment prior to their use in the election process to ensure that software is working as intended. For electronic voting machines, this means that all machines are accurately recording votes as cast. To ensure public confidence, parties and civil society actors should be allowed to monitor the testing and the results of the testing process must be made public.
- Use a chain of custody system for recording which officials have had access to the EETs and for what specific period of time to ensure the accountability of the system and those who had access to it.
- Monitor all EET systems as they perform their electoral functions to prevent, detect and respond to any cybersecurity attacks and any system malfunctions.
- Information gathered by EETs should be made available as open data in a timely manner, in accordance with legal safeguards for privacy and data security. This should include data on delimitations of constituency boundaries and voting precincts, lists of polling stations and their locations, information on ballot qualification of political parties and candidates, as well as voter registry and electoral results data.

Post-election

- Immediately after their use, and in line with the legal requirements, conduct audits of any EETs used for voting, results tabulation and results announcement. Such auditing processes should be accessible for observation and verification by political contestants and civil society election observers, and the results be made public.
- Adequately maintain EET equipment including through regular software and antivirus program updates. Store equipment in a safe location that complies with any temperature or other environmental requirements.

Parliaments

A country's legislature has an important role in ensuring the inclusion, transparency and accountability of election processes. It defines the electoral system that translates citizens' votes into political power, provides an overall framework for the conduct of elections, and allocates the funding for the election authorities to perform their work. When considering the introduction of new EETs, parliaments should ensure that the legal framework and available funding enable the EMB to implement the recommendations presented above.

- Conduct, in partnership with the EMB, a broad consultative process on whether to introduce EETs that is inclusive of political and civil society actors and takes into account the widest possible spectrum of opinions.
- Following the decision to introduce EETs, pass the necessary legislation and amendments, including the allocation of sufficient funding, to ensure that the electoral process can be conducted with certainty and in accordance with the principles of inclusion, secrecy,

integrity, universality, equality, transparency, accountability, security and public confidence. This should include ensuring that tendering and procurement for EET solutions is done in line with the national public procurement and anti-corruption frameworks based on transparency, competition and objective criteria in decision-making.

- Ensure that the legislative framework provides that the national electoral authorities retain full ownership and control over all aspects of the electoral process and that the EMB has ownership over all the data captured, managed or produced by the EET system as well as all operational aspects of the system, including the collection and storage of data, so that it is subject to the country's legal jurisdiction and requirements.
- In consultation with relevant experts and institutions, define the standards for certification of EETs, such as electronic voting machines. Standards should include international key principles for the implementation of EETs and may also include technical specifications for EET equipment. They may also refer to existing standards that need to be respected, such as data protection and cybersecurity. Dialogue around the definition of standards should include the expert community, civil society, political actors and voters.

Electoral dispute resolution bodies

The introduction of EETs can pose special challenges for bodies responsible for resolving electoral disputes. In some cases, the technology could make the process less transparent and make it more difficult to assess the merits of a claim. For example, electronic voting machines that do not produce a paper trail make it impossible to conduct audits to assess whether votes were counted as cast. In addition, the introduction of technology requires these bodies to identify or develop technical expertise to better understand how the systems work and potential implications for electoral integrity.

- Consider how the application of rules of evidence, procedure, and other jurisprudential matters may be challenged by the technical complexity of issues that may be raised concerning EETs within the timeframes required for electoral disputes.
- Take steps to ensure that tribunals and other relevant bodies are prepared to process such disputes, including any specialized training, identification of appropriate expertise, designation of jurisdiction for such disputes, and public notification of such matters.

Specialized national agencies

Different government agencies could play an important role in the introduction of EETs. For example, anticorruption agencies can provide guidelines and oversight during the procurement processes. Other agencies can provide relevant technical expertise to ensure that the selected EET solution complies with existing regulations and does not introduce substantial risks to the integrity of the elections. For example, agencies tasked with cyber security can help ensure that the selected EET is not open to hacking or other cyber attacks. Data protection agencies can verify that the system treats personal and other sensitive information in accordance with national legislation and

international best practices. They can also assist the EMB in ensuring transparency while protecting sensitive information.

- Lend expertise to the EMB during the more technical phases of implementation of EETs, including: defining the necessary technical specifications for the procurement process, testing, certification of the system and subsequent regular audits.

Political parties and candidates

Political actors contesting an election have an interest to ensure that the introduction of new EETs does not create an undue electoral advantage, introduce new barriers to the participation of their supporters, or reduce the transparency of the process. Political contestants should develop technical expertise to understand the implications of any new technology, and update their organizational and political strategy accordingly.

- Adjust party strategies to take into consideration the introduction of EETs. Consider hiring technical experts to advise on the process and otherwise expand the party's expertise to engage productively around the adoption and implementation of EETs. Participate actively in consultations with the EMB, parliament and civil society actors about the introduction and implementation of EETs.
- Prepare party poll-watchers (agents) to effectively observe EETs through specialized training and development of observation tools. Parties should focus in particular on what type of evidence is necessary to support the proper lodging of complaints involving EETs, and the means of documenting and communicating it to the public and the proper authorities.
- Prepare party legal teams concerning the procedural requirements for lodging complaints concerning EETs, the evidentiary requirements concerning such complaints, the types of redress to seek, and the related timeframes for adjudication.

Civil society

Civic activists monitor election and political processes to ensure that they represent the interests of citizens. Anticorruption monitors have a role in monitoring that the adoption of new EETs does not create opportunities for financial or political corruption. Citizen election observers can accompany and assess the design, testing and introduction of the technology solution, and their performance and impact during the elections.

- Participate actively in initial discussions and public consultations about the potential introduction of EETs and scrutinize the potential impact on civil and political rights.
- Develop specialized skills to give meaningful input into initial deliberations and public consultations, to be able to effectively monitor EETs during the election process, and to collect the necessary evidence to support findings.

- Monitor the EMB's activities at each phase of the introduction and implementation of EETs, including the procurement process, tests and pilots, and bring any concerns to the attention of the public.
- Actively inform the public about the nature of the issues concerning the potential adoption of EETs, their procurement and their implementation, to help build warranted public confidence and electoral accountability concerning their application.

Vendors

Companies or other entities providing technology for the administration of elections are responsible to ensure that the design of EETs adequately solves the problems that a country's EMB is trying to address, and that its testing, implementation and roll out are consistent with the principles described in this paper. Vendors' policies – for example, on licensing structures or data ownership – can also impact the longer term sustainability of the EET.

- Demonstrate their commitment to respecting international human rights principles for democracy and electoral integrity when considering the development, marketing and implementation of EET systems.
- Carry out a process of human rights due diligence² before deciding to provide an EET system, as defined by the United Nations Guiding Principles for Business and Human Rights. Given the importance of an electoral system to the democratic institutions of a country, stringent requirements of due diligence should be applied. Impact assessments should ensure that any EET complies with do-no-harm and sustainability principles.
- Consider how EET systems can be designed that embed fundamental election principles, increasing the likelihood they will be respected when the system is operating. For instance, a VVPAT (voter verifiable paper audit trail) produces a paper record that can be checked by the voter to make sure their vote is accurately recorded. End-to-end verification systems allow electoral authorities and contestants to confirm that all votes have been accurately recorded and tabulated.
- Structure their relationship with election authorities to ensure that election officials have ultimate ownership of the election process and the resulting data, including voter registries and granular election results. The data should be available to the election authorities in machine readable format that could be published as open data as appropriate and allowed by law, and that access to data is available to the jurisdiction of the respective national dispute resolution bodies.

² The concept of human rights due diligence is a critical part of fulfilling the “corporate responsibility to respect” as defined in the UNGPs. Human rights due diligence refers to the processes that all business enterprises should undertake to identify, prevent, mitigate and account for how they address potential and actual impacts on human rights caused by or contributed to through their own activities, or directly linked to their operations, products or services by their business relationships.

International donors and technical assistance provider

Often, national budgets are insufficient to facilitate the introduction of needed EETs. In some cases, bilateral or multinational international donors are able to provide the needed financial support. In other cases, international nongovernmental organizations are able to provide technical assistance to EMBs, parliaments and other entities both on the implementation of the EETs, and on the necessary adaptation of related processes such as electoral dispute resolution. In providing this assistance, international actors have the responsibility to ensure that the technology they are supported – and the process to introduce it — is consistent with the principles outlined in this document.

- Ensure that where EETs are funded as part of democracy support, the introduction of new technologies respects democratic principles and promotes human rights, including civil and political rights.
 - Ensure that donor-financed decisions to adopt EETs and their procurement of such technological solutions is done according to national laws and international standards for inclusion, in full transparency, and is followed by the adoption and testing of the EET system as well as its gradual introduction, training of stakeholders and effective voter education.³
 - While the introduction of EETs remains a sovereign decision for the EMB and national stakeholders, donors should only finance solutions that are compatible with fundamental principles for democratic elections, due diligence and ethical design, including equality, universality and related accessibility. These should provide strong guarantees in terms of functionality, security and of preserving the EMB's sovereignty over the electoral process.
- Bridge the skills gap by supporting EMBs, parliaments, political parties, and civil society actors to make inclusive decisions about whether to introduce EETs including, in addition to the principles noted above, the sustainability of the system in terms of implementation, management, maintenance and long-term cost.
 - Provide expertise through electoral assistance to help and accompany the EMB and other stakeholders in the decision-making process, as well as in the testing and introduction of EETs.
 - Support thorough feasibility assessments, including risk, cost and sustainability assessment in an inclusive process before any decision to proceed. Ensure that inclusive analysis is provided to identify the most effective technology to respond to identified challenges and the socio-economic context.

³ In cases where a specific donor, for instance the EU, finances the procurement, additional specific considerations related to the donor should be considered, for instance that EU standards for electronic identity, cybersecurity and data protection be included in the procurement.

- Provide support to political parties, civil society actors and the EMB, including for technical assistance and development of national expertise, to monitor and verify the processes around and the functioning of EETs to establish accountability and effectively communicate with the public so that it may be confident in the integrity of the election process.
- Consider potential compatibility with initiatives aimed at ensuring transparency of governance systems, codes of good practice and other initiatives that strive to promote transparency, such as the Open Data initiative.⁴ This initiative has also been adapted to cater for elections through the Open Election Data Initiative,⁵ launched by NDI, which sets principles, and training modules for EMBs, observers and others.

Conclusion

The introduction of new technologies in elections is not a simple or quick process. It requires the concerted efforts not only of the election authorities, but also of a broader range of stakeholders, from legislators to government agencies to civil society. Each of these actors has a responsibility to ensure that the introduction of EETs is consistent with the principles of inclusion, secrecy, integrity, universality, equality, transparency, security and public confidence.

As new EETs are introduced in elections around the world, the recommendations can provide guide posts for each stakeholder, and a model that international and citizen observers can use as they develop their own recommendations based on the findings of their observation.

⁴ The six charter principles were developed in 2015 by governments, civil society, and experts around the world to represent a globally agreed set of aspirational norms for how to publish data. <https://opendatacharter.net/principles/>

⁵ <https://openelectiondata.net/en/>