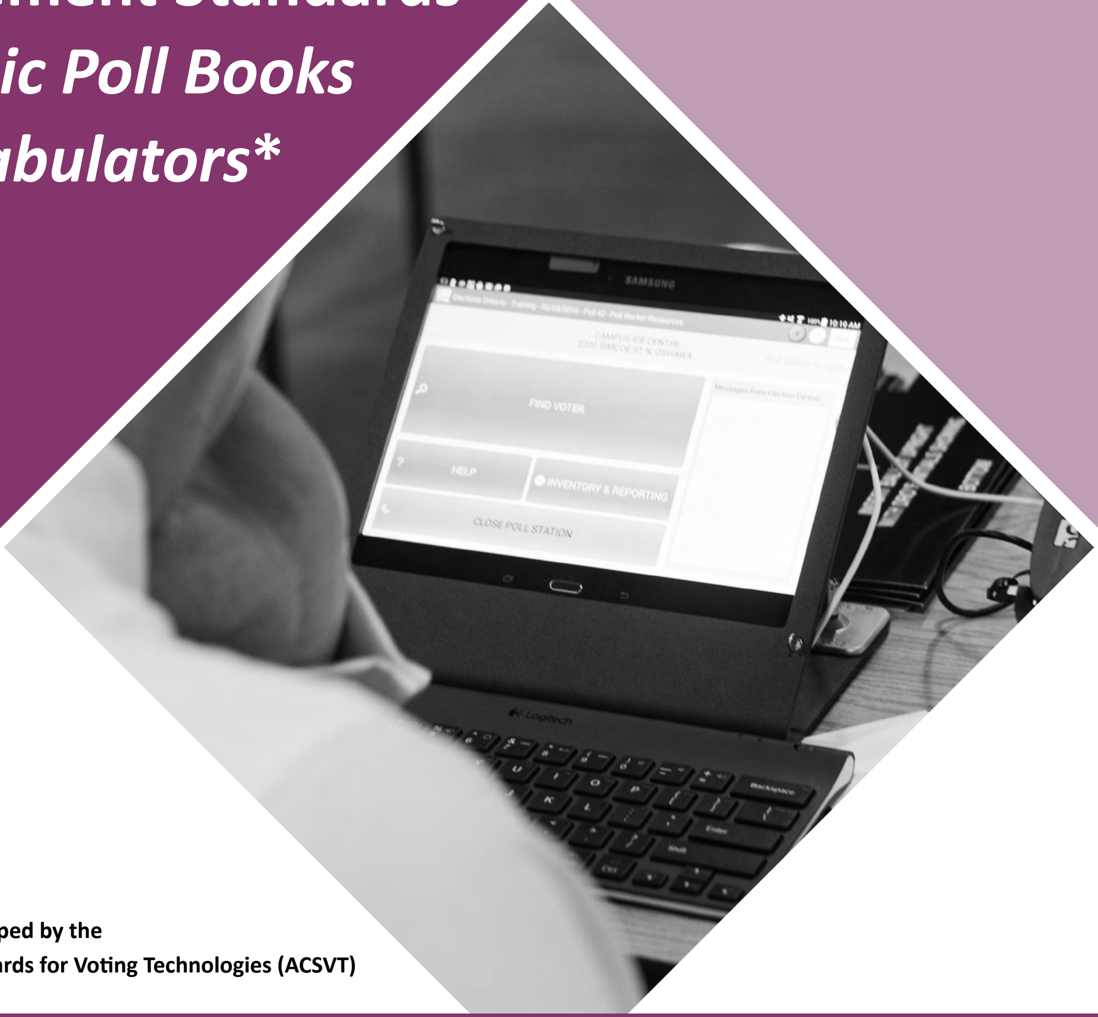
Recommendations for Management Standards on *Electronic Poll Books* and *Vote Tabulators**



* Management Standard developed by the Advisory Committee on Standards for Voting Technologies (ACSVT)

Table of Contents

Advisory Committee on Standards for Voting Technologies Background

The Advisory Committee on Standards for Voting Technologies (ACSVT) was created by the Chief Electoral Officer of Ontario. The structure and mandate of the ACSVT were devised in accordance with amendments made to Ontario's *Election Act* through Bill 254, *Protecting Ontario Elections Act, 2021.* The ACSVT was mandated to make recommendations on standards for voting equipment and vote counting equipment currently in use in Ontario provincial elections. The committee's scope focused on *electronic poll books* and *vote tabulators.*

The ACSVT was made up of individuals chosen by each political party in the Legislative Assembly of Ontario and three members appointed by the Chief Electoral Officer. Appendix 1 provides a detailed overview of all ACSVT members.

Since the establishment of the ACSVT in August 2021, the committee developed the following principles to help guide the standards development process:

1. Democratic Election Principles;
2. Technical Design Principles: Voting Technologies; and
3. Technical Design Principles: Election Technologies.

A comprehensive list of the guiding principles can be found in Appendix 2. These principles were developed solely to guide the development of these Standards and are not intended to be read as part of the Standards, or to be considered more broadly applicable. They are provided in the Appendices for the purposes of transparency.

Recommendations for Management Standards on Electronic Poll Books and Vote Tabulators

1 Scope

As defined in Bill 254, *Protecting Ontario Elections Act, 2021,* this Standard was developed by the ACSVT with the support of the Digital Governance Standards Institute (DGSI) for provincial elections in Ontario. While it does not directly apply to other jurisdictions, it may be adopted by other *electoral management bodies* with minor amendments. It may be used as guidance for any *electoral management body* as it is technology neutral but may not be fully applicable due to legislative differences between jurisdictions. This Standard does not replace legislative requirements, existing standards, certifications, policies, or processes which, at the present time, allow organizations to conduct *elections.* This Standard does not affect the independence of the Chief Electoral Officer, as it is voluntary. As such, the requirements are written in a manner to demonstrate compliance.

There are various legislative, policy, and operational instruments that impact how provincial *elections* are conducted in Ontario. At the highest level is the *Election Act,* and case law interpreting the legislation. The *Election Act* defines requirements that must be met when administering an *election* event (from planning to post election). Examples of requirements set out in the *Election Act* include *vote counting,* registration requirements for *electors,* the rights and duties of *scrutineers,* and the powers of the electoral authority. Other applicable legislation is also referenced throughout this Standard.

Ontario provincial *election administrators* shall continue to take into consideration the impact on all *stakeholders* when using *electronic poll books* and *vote tabulators* in *elections.* These assessments ensure that Ontario *election administrators* meet the requirements set out in Section 4.4.(2) of the *Election Act* when introducing modifications to the voting process:

1. Improve the voting process for *electors.*
2. Achieve administrative efficiencies.
3. Maintain the integrity of the voting process.

The purpose of this Standard is to specify the baseline operational requirements where the province of Ontario:

- intends to run a democratic *election* using *electronic poll books* and *vote tabulators;*
- needs to demonstrate its ability to manage *elections* by secret *ballot,* to provide reliable, transparent, free, and fair results that comply with electoral requirements; and
- aims to enhance the trust and confidence of citizens, candidates, political organizations, and other electoral interested parties.

This Standard is based on the foundation built by Elections Ontario in its administration of *electronic poll books* and *vote tabulators* since they were first piloted. Other useful documents developed by electoral agencies outside of Canada, such as the Electoral Assistance Commission and the Council of Europe, were valuable resources during the creation of this Standard.

This Standard leverages the policies and protocols already put in place by Elections Ontario to create the first formalized voluntary guide in Canada with input from across Canadian *electoral management bodies.* This Standard provides outcome-based recommendations that are intended to aid those who oversee provincial *elections* in Ontario as they continue to set out their directives, policies, and operational guidelines created under the Chief Electoral Officer's powers under the *Election Act.* These recommendations are applicable to the entire *election* period, including pre-*election* and post-*election* activities or processes. In the event of a conflict, inconsistency, or a discrepancy between the *Election Act* and these recommendations, the provisions in the *Election Act* are paramount as the governing law.

This document separates the recommendations into three categories. They are organizational infrastructure; access and usability; and security and integrity; as these are the areas that are most impacted by the introduction of *electronic poll books* and *vote tabulators.* While this document covers both *electronic poll books* and *vote tabulators,* they serve different functions, and some clauses may apply to one but not the other.

The ACSVT acknowledges that a rigorous security engineering lifecycle shall be developed to achieve a robust security framework. A security engineering lifecycle is "the use of established and rigorous engineering processes to the verifiable fulfillment of documented security requirements and protection needs, applied throughout program management, development, acquisition, manufacturing, fabrication, production, operations, sustainment, training, retirement, and disposal of a system" (Ross, R., Winstead, M., & McEvilley, 2022). Security relating to the broader engineering lifecycle and corporate governance are procurement related and include contractual requirements mandated under a Government of Ontario procurement process. For the purposes of the development of this Standard, these are considered outside the scope of the legislative mandate of the ACSVT.

Finally, the recommendations included in this Standard do not provide guidance for specific vendor technology solutions. Rather they are technology neutral and provide guidelines on the functions that are performed within those technology solutions. It is also important to note that it remains the responsibility of any other *election management body* considering these recommendations to judge their suitability for application within their own jurisdiction.

Product Standards for *electronic poll books* and *vote tabulators* have been developed and provide the technical design requirements. Refer to DGSI 119-1, *Election and Voting Technologies – Part 1: Vote Tabulators* for the *Vote Tabulator* Product Standards and DGSI 119-2, *Election and Voting Technologies – Part 2: Electronic Poll Books* for the *Electronic Poll Book* Product Standards.

2 Conformance Language

This Standard distinguishes the use of specific keywords such as "shall" and "should" or "must" and "may" to enhance clarity. Refer to Appendix 3 where additional details pertaining to these terms have been outlined.

3 Normative References

The following references, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

- *DGSI 119-1, Election and Voting Technologies – Part 1: Vote Tabulators*
- *DGSI 119-2, Election and Voting Technologies – Part 2: Electronic Poll Books*
- *ISO 31000:2018 Risk Management – Guidelines*
- *GO-ITS 25.0 General Security Requirements*
- *Elections Ontario Integrated Accessibility Standards Policy*
- *Elections Ontario Identification Policy*

NOTE: See Glossary in Appendix 4 for additional information on these standards and their accompanying organizations.

4 Terms and Definitions

administrator

A privileged user of a *vote tabulator* or and *electronic poll book (hardware/software)* with the highest level of access to configure or administer system functions.

[SOURCE: NIST election terminology glossary], modified.

authorization

Granting of rights, which includes the granting of authorized access based on pre-defined criteria.

[SOURCE: ISO 7498-2:1989, 3.3.10].

assistive voting equipment

The assistive devices provided by the Chief Electoral Officer, which mark a *ballot* in the designated space beside a candidate's name, after an *elector* has followed prompts and selected a candidate by:

(1) sip and puff device, or
(2) paddle interfaces, or
(3) audio tactile interface.

[SOURCE: Elections Ontario's Directive for the 2022 General Election for all electoral districts for vote counting equipment and accessible voting equipment].

ballot

A physical presentation of the *contest* options for a particular *voter.*

[SOURCE: *Voluntary Voting System Guidelines* (VVSG) 2.0.].

ballot style

A unique *ballot* that may be issued in an *election,* that contains a unique set of one or more *contests* that a particular group of *electors* are entitled to receive.

cast vote record

A *cast vote record* (CVR) is an electronic record of a *voter's ballot* selections.

Note: For clarification purposes, the overall record of the *ballots* for an *election* includes the physical *ballots* for an *election.*

[SOURCE: NIST SP 1500-103], modified.

contest

A single decision or set of associated decisions being put before the *voters.* This term encompasses other terms such as "race," "question," and "issue" that are sometimes used to refer to specific kinds of contests. It does not refer to the legal challenge of an *election* outcome.

[SOURCE: *Voluntary Voting System Guidelines* (VVSG) 2.0.], modified.

election

Means an *election* of a member or members to serve in the Legislative Assembly.

NOTE 1: For the purpose of this document, "*election"* also refers to the following: *contest,* by-*election,* referendum, etc.

NOTE 2: For the purpose of municipalities who may choose to adopt this Standard, *"election"* would also refer to electing members of its government body such as a municipal council.

[SOURCE: Ontario *Election Act,* R.S.O. 1990, c. E.6, s. 1].

election official

Any person who is authorized with administering or conducting an *election,* including temporary *election* workers.

[SOURCE: *Voluntary Voting System Guidelines* (VVSG) 2.0.], modified.

elector

A person who is entitled under the *Election Act* to vote in an *election* for the Legislative Assembly of Ontario.

NOTE: For the purposes of other jurisdictions who choose to adopt this Standard, the legislation and governing body would be amended to reflect that jurisdiction.

[SOURCE: Ontario *Election Act,* R.S.O. 1990, c. E.6, s.1], modified.

electoral management body

Public institution having legal and administrative responsibility for the preparation and conduct of *elections* according to the legal framework of the jurisdiction (e.g., country/province/territory/municipality/organization).

[SOURCE: ISO/TS 54001:2019 – Quality management systems — Particular requirements for the application of ISO 9001:2015 for electoral organizations at all levels of government], modified.

electronic poll book

An electronic device running or accessing a software application that manages the approved *voters' list* for an electoral region. It is used by an *election official* to look up, validate, register, and check-in individuals who present themselves to vote.

[SOURCE: Canadian Centre for Cyber Security, *Security Considerations for Electronic Poll Book Systems,* 2022], modified.

electronic poll book hardware

Refers to a device on which an *electronic poll book software* is installed, such as a laptop, tablet, or mobile device.

electronic poll book hardware manufacturer

The producer of a purpose-built *electronic poll book (software* and *hardware)* to facilitate the electronic check-in of *voters* at polling locations during *elections.*

electronic poll book software

Special purpose digital application designed to facilitate *voters'* information during an *election.* It runs on devices such as laptops and tablets and offers various functionalities including documenting IDs and enabling updates to *voter* records, ensuring accurate and up-to-date information, allowing *election official*s to verify *voters'* eligibility, and implementing security measures to safeguard voters information and preventing *unauthorized access.*

[SOURCE: U.S. Election Assistance Commission].

electronic poll book software developer

The developer of a software solution for the *electronic poll book.* The software developer provides an application that manages the approved *voters' list* for an electoral region.

firmware

A specific class of software encoded directly into a hardware device that controls its defined functions and provides the low-level control for the device's specific hardware (such as the *firmware* that initially boots an operating system).

[SOURCE: *Voluntary Voting System Guidelines* (VVSG) 2.0.].

logic and accuracy (L&A) testing

Equipment and system readiness tests whose purpose is to detect malfunctioning devices and improper *election*-specific setup before the equipment or systems are used in an *election. Election officials* conduct *L&A tests* on all *ballot* designs prior to the start and end of an *election,* as part of the process of setting up the system and the devices for an *election* according to jurisdiction practices and conforming to any local laws.

[SOURCE: NIST Election Terminology Glossary], modified.

multi-factor authentication

Authentication that uses a combination of two or more different authentication factors – something a *user/operator* knows (e.g., a password), has (e.g., a physical token), or is (e.g., a biometric) – to verify a *user/operator's* identity.

[SOURCE: CAN/DGSI 104:2021 Baseline cyber security controls for small and medium organizations], modified.

nonconformities

Failure to meet one or more requirements that are outlined in the mandatory clauses.

[SOURCE: IS0 9001].

overvote

Occurs when the number of selections made by a *voter* in a *contest* is more than the maximum number allowed.

[SOURCE: *Voluntary Voting System Guidelines* (VVSG) 2.0.].

permissions

Set of rules which describe what a user or group of users may access or control within a system.

[SOURCE: ISO/IEC 18598:2016, 3.1.29].

real-time

Quality of a process, the execution of which is determined or controlled in time. The term is sometimes extended to refer to a delivery process which is perceived fast enough to be considered as almost instantaneous (e.g., current, updated).

[SOURCE: ISO/IEC TR 16501:1999].

results tape

The *vote tabulator's* printed report which shows the total number of votes cast for each candidate or for each option in a *contest.*

risk limiting audit

Post-*election tabulation* audit procedure for checking a sample of *ballots* (or *elector* verifiable records) that is guaranteed to have a large, pre-specified chance of correcting the reported outcome if the reported outcome is wrong (that is, if a full hand count would reveal an outcome different from the reported outcome).

[SOURCE: *Voluntary Voting System Guidelines* (VVSG) 2.0.].

scrutineer

A person appointed by a candidate, who represents them at a voting location to observe the voting and the counting of *ballots* and scrutinize its integrity and fairness. The *scrutineer* may raise objections to be determined by the *election official* responsible for the particular function where the objection is raised.

[SOURCE: Elections Ontario Glossary], modified.

stakeholder

Individual or organization, having an interest in a system such as *electors,* political entities, and *election officials.*

[SOURCE: NIST SP 800-160v1r1], modified.

system integrity

The *electronic poll book* and *vote tabulator system* performs its intended function in an unimpaired manner, free from *unauthorized access,* or manipulation of the system (intentional or accidental).

[SOURCE: *Voluntary Voting System Guidelines* (VVSG) 2.0.

tabulation

The electoral process for *vote counting.*

[SOURCE: ISO/TS 54001:2019 – Quality management systems — Particular requirements for the application of ISO 9001:2015 for electoral organizations at all levels of government], modified.

test deck

A set of marked *ballots* with a predetermined outcome. Used for *logic and accuracy testing* of a *vote tabulator* or assistive voting technology (*ballot* marking devices).

[SOURCE: NIST, "Election Terminology Glossary"], modified.

unauthorized (access, disclosure, use)

Access to physical or logical network, system, sub-system, or data without *authorization* and/or authentication. An incident affecting the confidentiality, integrity, or availability of data. Use of a physical or logical network, system, or data without *permission.*

[SOURCE: CAN/DGSI 104:2021 Baseline cyber security controls for small and medium organizations], modified.

undervote

Occurs when the number of *voter* selections in a *contest* is less than the maximum number allowed for that *contest* or when no selection is made. The number of *undervotes* is equal to the number of votes lost, for example, if no selection is made in a vote for two *contests* the number of votes lost is two.

[SOURCE: *Voluntary Voting System Guidelines* (VVSG) 2.0.], modified.

USB (universal serial bus)

Serial system for connecting a computer with external devices.

[SOURCE: ISO 2789:2022(en), 3.3.59].

user/operator

Personnel, such as *election officials,* who operate *vote tabulators* and *electronic poll books* to support pre-*election* and *election* preparation, post-*election* activities, and polling place activities, as applicable, with regard to all *electronic poll book* and *vote tabulator* functions.

vote counting

Counting of the *ballots* at poll locations.

[SOURCE: ISO/TS 54001:2019 – Quality management systems — Particular requirements for the application of ISO 9001:2015 for electoral organizations at all levels of government].

vote tabulators

Single-function, purpose-built devices used by an *electoral management body* to scan paper *ballots,* tabulate votes, print a *results tape,* and create a *cast vote record.* For the purpose of this document, the *vote tabulator* includes any peripheral *ballot* box to which it is sealed as *ballots* are cast.

[SOURCE: ISO/TS 54001:2019 – Quality management systems — Particular requirements for the application of ISO 9001:2015 for electoral organizations at all levels of government], modified.

vote tabulator system

The total combination of mechanical, electromechanical, or electronic equipment (including the software, *firmware,* and documentation required to configure, control, and support the *vote tabulator)* that is used to define *ballot styles;* count votes; to report or display *contest* results; to maintain and produce any audit trail information; and the practices and associated documentation used to identify system components and versions of such components; to test the system during its development and maintenance; to maintain records of system errors and defects; to determine specific system changes to be made to a system after the initial qualification of the system.

[Source: United States Election Assistance Commission].

vote target area

The defined area on the paper *ballot* in which the *voter* must make their marks in order to be detected by the *vote tabulator* as a valid mark and be countable as a vote.

voter

An *elector* who has appeared at a polling place and has accepted a *ballot* for marking which has been placed in the ballot box or has declined their *ballot* and so declared.

[SOURCE: Ontario *Election Act,* R.S.O. 1990, c. E.6, s.1].

voter information/data

Collection of personal information and data on registered *voters.*

[SOURCE: Canadian Centre for Cyber Security, *Security Considerations for Electronic Poll Book Systems,* 2022], modified.

voters' list

Approved list of *electors* for a particular polling area.

[SOURCE: *Canadian Centre for Cyber Security, Security Considerations for Electronic Poll Book Systems,* 2022], modified.

5 Organization Infrastructure

5.1 Organizational Capacity

The introduction of *electronic poll books* and *vote tabulators* requires a skilled labour force, which needs to be trained and equipped with the necessary tools and resources to perform their duties. Although fewer individuals are required to work at the poll, *election officials* require competencies that are more technical in nature.

Provincial *elections* in Ontario need to build the necessary capacity to effectively oversee the *election* in accordance with legal requirements, without being dependent on private parties (whether commercial or not-for-profit).

Ontario should implement the following when adopting *electronic poll books* and *vote tabulators* into their *election* delivery model:

5.1.1 Build and maintain the necessary capacity, and related technical competencies, through its hiring practices and robust training for staff at every step of the electoral process in the use of *electronic poll books* or *vote tabulator* solutions.

5.1.2 Include provisions in contractual agreements with third parties and their subcontractors, when outsourcing any part of the electoral process to ensure they meet all legislation and fulfill standards set out by Ontario.

5.1.3 Develop policies that outline the division of duties (roles and responsibilities) between Ontario and any third-party vendor.

NOTE: There are some activities that should not be undertaken by the technology vendor, such as conducting audits, etc.

5.1.4 Ensure that processes are controlled and transparently documented in a form suitable for methods of operations in provincial *elections* in Ontario.

5.2 Risk Management

The use of *electronic poll books* and *vote tabulators* introduces unique challenges resulting in more complexity in identifying risks in the electoral process. Risk management specific to *electronic poll books* and *vote tabulators* should be developed within the organization's broader risk management framework and cover activities related to the development, implementation, operation, and maintenance of the technology solution. Addressing both risks and opportunities establishes a basis for achieving improved results and preventing negative outcomes. Conducting continuous risk management based on predefined criteria for risk acceptance and a predefined methodology such as those found in ISO 31000:2018 is important to ensure the security and integrity of the *election.*

Ontario shall implement the following when adopting *electronic poll books* and *vote tabulators* into their *election* delivery model:

5.2.1 Adopt a continuous risk management approach specific to the implementation of *electronic poll book* and *vote tabulators* (as the technology evolves and/or as new technology emerges over time) into their *election* delivery footprint and include the following activities:

a. identify criteria for assessing risks and threats;

b. identify actions to prevent or mitigate the identified risks and threats;

c. monitor the reliability and usability of the equipment as it ages including analyzing the life expectancy of the voting system;

d. identify and assess all *nonconformities* (such as non-compliance by *election officials* on any policy or procedure);

e. take action to prevent recurrence that is appropriate for the effects of the *nonconformity;* and

f. communicate effectively (clear, concise, correct, concrete, timely) to affected, within the organization's broader communication strategy.

5.2.2 Ensure risk strategies are reviewed prior to an *election* and are applied to all phases of the *election* cycle.

5.2.3 Identify scenarios requiring contingency planning, develop and test contingency processes to address these scenarios, and determine decision-making authority to implement the contingency processes.

5.2.4 Ensure *election officials* are trained effectively on when and how to activate/deactivate contingency plans.

5.2.5 Develop a support model for the use of *electronic poll books* and *vote tabulators* that includes:

a. on-site support at polling places;
b. decision making processes;
c. issues escalation processes;
d. communication protocols;
e. vendor support models; and
f. secure handling procedures during storage and transportation.

5.3 Monitoring, Measurement, Analysis, and Evaluation

As part of its commitment to continuous improvement, Ontario provincial *elections* should incorporate *electronic poll books* and *vote tabulators* as a component of its broader organizational evaluation program, that includes post-*election* reporting as required under the *Election Act* (s 67.2). Continually assessing the suitability, adequacy, and effectiveness of the use of *electronic poll books* and v*ote tabulators,* will result in improved products and services to better meet the organization's stated objectives, as well as to address future needs and expectations of all *stakeholders.*

Ontario should implement the following when adopting *electronic poll books* and *vote tabulators* into their *election* delivery model:

5.3.1 Develop a program to evaluate the performance and the effectiveness of the use of *electronic poll books* and *vote tabulators* during an *election*, including, but not limited to, the time it takes to complete an addition of an *elector* in an *electronic poll book*, the time it takes for a *ballot* to be scanned by the *vote tabulator*, and the time it takes for an *elector* to move through the poll and complete the voting process.

5.3.2 Provide a process for all *voters,* including persons with disabilities, to provide formal feedback on their voting experience with technology at the polling place.

5.3.3 Prior to any *election,* create and implement, or review and update, the program to assess the use of *electronic poll books* and *vote tabulators* and include the following:

a. all activities to be monitored, measured, and reported;

b. establish methodology to monitor, measure, analyze and evaluate;

c. establish methodology to obtain feedback from all *stakeholder* groups;

d. identify the timing of when monitoring and measuring will be performed;

e. identify the timing of when monitoring and measurement will be analysed, evaluated, and reported; and

f. identify opportunities to implement recommendations/enhancements/improvements based on evaluations.

NOTE: This evaluation process should provide a report on how practices and policies will be modified based on the lessons learned and standards adopted to ensure continuous improvement of the *election* process.

6 Access and Usability

6.1 Access

One of the primary benefits associated with the adoption of *electronic poll books* and *vote tabulators* is the ability to improve access. It is recognized that there are other factors to be considered in the decision to adopt *electronic poll books* and *vote tabulators.* These include operational efficiencies, and the ability to improve the integrity of *election* administration by reducing administrative errors. Ontario provincial *elections* need to balance these considerations when assessing how best to use *electronic poll books* and *vote tabulators* to improve access for all *electors* in Ontario.

Ontario shall implement the following when adopting *electronic poll books* and *vote tabulators* into their *election* delivery model:

6.1.1 Ensure that the *electronic poll books* and *vote tabulators* meet the accessibility needs of all *stakeholders*.

6.1.2 Leverage, where possible, opportunities to implement *electronic poll books* and *vote tabulators* across the province including such polls as hospitals and remote/fly in communities ensuring equal access to voting and general deployment across the province.

6.1.3 Ensure that the design and implementation of *electronic poll books* and *vote tabulators* maintains or improves the level of transparency; political entities' ability to scrutinize electoral proceedings; levels of detail of reporting; meaningful reporting of results; and the public's ability to review and analyze the results.

6.2 Accessibility for Persons with Disabilities

Ontario is required to comply with accessibility legislation such as the *Charter of Rights and Freedoms,* the *Ontario Human Rights Code,* the Ontario *Election Act,* and the *Accessibility for Ontarians with Disabilities Act.*

In addition, the *Election Act* includes several requirements to ensure the *election* process is accessible to all *electors.* Elections Ontario continues to assess and improve accessibility in the *election* process, including *assistive voting equipment* (including, but not limited to equipment such as sip and puff, paddle interface, or audio tactile interface) at all returning and satellite offices during advance voting and on *election* day. Should a *voter* choose to cast their *ballot* outside of a returning or satellite office during the advance vote period or on polling day, they are able to do so through several other accessible channels including vote-by-mail, home visit, or hospital visit.

Ontario shall implement the following when adopting *electronic poll books* and *vote tabulators* into their *election* delivery model:

6.2.1 Formally facilitate consultations with representatives of disability *stakeholder* groups to ensure that the services provided to persons with disabilities address their access needs.

6.2.2 Develop policies and procedures to ensure *electronic poll book* and *vote tabulators* are accessible to *electors* and *election officials* with disabilities. These practices must meet Ontario accessibility standards, such as the *Accessibility for Ontarians with Disabilities Act* and Integrated Accessibility Standards (Ontario Regulation 191/11). In addition, these must also comply with Elections Ontario's requirements and commitments contained in their Accessibility Program.

6.2.3 Develop and provide accessibility training to all *election officials* and third parties providing services to *electors* and *voters*.

6.2.4 Develop clear and accessible instructions and information in all applicable accessible formats on how *electors* can access *assistive voting equipment.*

6.2.5 Ensure that *election officials* are provided with clear, complete, and detailed instructions and messages for setup, check-in, shutdown, and how to use accessibility features on the *vote tabulators* including *assistive voting equipment.*

6.2.6 Ensure all *electors* receive equivalent information and options in all modes of voting.

NOTE: The *ballot* should be presented to the *elector* in a manner that is clear and usable. An *elector* must be able to understand the *ballot* presentation easily and independently of their abilities. *Electors* should encounter no difficulty or confusion regarding the process for marking their selections.

6.2.7 Ensure that *electronic poll books, vote tabulators,* and *assistive voting equipment* are accessible in a manner that provides the same opportunity for access and participation (including privacy and independence) for all *electors*.

6.3 Usability

Usability is defined generally as a measure of the effectiveness, efficiency, and satisfaction achieved by a specified set of users with a given product in the performance of specified tasks. The core design principles of usability focus on: if the design is intuitive, if it is easy to learn, if it is efficient, and if it satisfies the *user/operator, voter.*

There are many ways to evaluate the usability of *electronic poll books* and *vote tabulators.* Common practices for collecting input from *voters* and *election officials* using the *electronic poll books* and *vote tabulators* include demonstrations, feedback surveys, and focus groups, and/or analyzing statistics from the technology in use (results analytics or statistics about access from a server). A best practice for evaluating usability is to observe *election officials* and *voters* using the system either as they work or in an environment set up for this purpose – called usability testing. Usability testing is a critical tool to ensure that *electronic poll books* and *vote tabulators* operate successfully in an *election.*

Ontario should implement the following when adopting, or modifying the use of *electronic poll books* and *vote tabulators* into their *election* delivery model:

6.3.1 Assess usability, including setting out the procedures it will use to assess usability tests conducted under *DGSI 119-1, Election and Voting Technologies – Part 1: Vote Tabulators* (*Vote Tabulator* Product Standard) and *DGSI 119-2, Election and Voting Technologies – Part 2: Electronic Poll Books* (*Electronic Poll Book* Product Standard) to help identify possible disenfranchisement, accessibility issues, operational issues, and general usability among *election officials* and *electors*.

NOTE: Usability tests generally include *electronic poll book* and *vote tabulator system* setup, operation during voting, and shutdown, with representative *election officials* and *electors,* to demonstrate that *election officials* can learn, understand, and perform these tasks successfully.

6.3.2 Ensure that information and instructions developed for *electors* and *election officials* are written clearly, following the best practices for plain language.

6.3.3 Ensure all *voters* have a consistent experience, as applicable, throughout the voting process that uses *electronic poll books* and *vote tabulators.*

NOTE: The voting process, for the purposes of these recommendations, includes access to the *electronic poll books* and *vote tabulators,* instructions on how to vote, initiating the voting session, making *ballot* selections, reviewing of the *ballot,* final submission of the *ballot,* and getting help when needed.

7 Security and Integrity

7.1 General

Public confidence in the integrity of *electronic poll books* and *vote tabulators* depends on the transparency of the *election* administration, hardware manufacturers, and software developers in relation to their security measures. This is important both for ensuring integrity in the underlying measures as well as building public confidence.

Security of *electronic poll books* and *vote tabulators* used in Ontario provincial *elections* rely primarily on the effectiveness of the controls in place to secure the supply chain, and the security of its hardware, software, network, and data.

The adoption of a robust organizational security framework is critical for the integrity of the *electronic poll books* and *vote tabulators* and should be consistent with government security standards more generally, such as the Ontario GO-ITS 25.0 *General Security Requirements* that defines minimum security standards to protect the integrity, confidentiality, and availability of networks and computer systems, or the Canadian government's ITSG-33 *IT Security Risk Management: A Lifecycle Approach.*

Ontario shall implement the following when adopting *electronic poll books* and *vote tabulators* into their election delivery model:

7.1.1 Ensure the use of *electronic poll books* and *vote tabulators* are compliant with the Ontario *Election Act.*

7.1.2 Adopt and document processes and procedures, including quality assurance testing, that ensure the *electronic poll books* and *vote tabulators* used in the voting process are secure and operate as intended.

NOTE: *Ballot* design programming requirements are set out in DGSI-119-1, *Election and Voting Technologies – Part 1: Vote Tabulators.*

7.1.3 Develop procedures to detect and correct any errors or unauthorised intervention with the *electronic poll books* or *vote tabulators,* including adopting *ballot* paper security features such as fibre signatures or watermarks, tamper-evident seals, and security check on tabulator prior to the zero-out.

7.1.4 Require that full maintenance of the *electronic poll book* and *vote tabulator systems* be conducted prior to their use in an *election* such as:

a. including documentation of a complete systems readiness test and proper programming of memory cards for the *vote tabulator;*

b. performing system maintenance;

c. performing upgrades and/or patches;

d. performing standard interface changes;

e. element replacement (e.g., spare part, alternate supply) and other activities to ensure the technology functions as intended; and

f. upgrades with any associated vulnerabilities.

NOTE: Testing to be conducted by a trained and qualified service technician to identify any existing or potential issues.

7.1.5 Ensure that there is a division of roles and responsibilities that are clearly defined and documented, so that a technology vendor does not undertake or participate in any oversight activity that is the responsibility of the *administrator* (e.g., conducting results auditing procedures). Where such activities are outsourced, that third-party must not include the technology vendor or any associated individual or organization.

7.1.6 Ensure that the design and implementation of *electronic poll books* and *vote tabulators* preserves the confidentiality, integrity, and availability of the *election* process.

7.2 Privacy

Privacy standards are critical to protect *voter information/data* from external access or internal misuse by requiring information only be accessed for the purpose as defined in the legislation and/or Elections Ontario's Privacy Policy.

Current privacy guidelines are defined in legislative requirements under the *Freedom of Information and Protection of Privacy Act* (FIPPA) that Elections Ontario voluntarily follows as well as best practices set out by the Information and Privacy Commissioner of Ontario, the Office of the Privacy Commissioner of Canada, and the ten privacy principles of the Canadian Standards Association.

Ontario shall implement the following when adopting *electronic poll books* and *vote tabulators* into their election delivery model:

7.2.1 Develop and integrate privacy policies and procedures for the *electronic poll book* into its broader privacy framework, that meet requirements in the *Election Act.*

NOTE: When developing privacy policies and procedures specific to the *electronic poll book,* those who oversee Ontario provincial *elections* should also take into consideration Ontario privacy laws, standards, and best practices, such as the Freedom of *Information and Protection of Privacy Act* (FIPPA) and the GO-ITS 25.0 *General Security Requirements.*

7.2.2 Ensure its privacy policies and procedures for the *electronic poll book* include Breach Management practices that cover the following:

a. incident management/reporting;
b. containment;
c. notification;
d. investigation;
e. remediation; and
f. lessons learned, and implementation of any recommended changes.

7.2.2.1 Conduct regular Privacy Impact Assessments for *electronic poll books* to identify risks based on core information principles including:

a. accountability;
b. consent;
c. limiting collection;
d. limiting use, disclosure, and retention; and
e. accuracy.

NOTE: These security safeguards should be appropriate to the sensitivity of the information; and openness for the policies and practices relating to the management of personal information.

7.2.3 Develop policies and procedures for the *vote tabulator* that ensure secrecy of the *ballot* that include:

a. using privacy devices such as privacy sleeves; and

b. ensuring that a *vote tabulator* cannot be used in a way that enables the choice of a *voter* to be made known.

NOTE: The voting process should preclude anyone from determining the content of a *voter's ballot* without the *voter's* cooperation. A *voter* and their *vote* must be protected during the entire voting process, including protection from physical discomfort, physical harm, loss of privacy, or loss of confidentiality.,

7.3 Disposal, Selling, or Renting of Equipment

The Ontario *Election Act* permits Elections Ontario to make *electronic poll books* and *vote tabulator* equipment, advice, staff, or other resources available to other *electoral management bodies* in Canada (2016, c. 33, s. 2.). Appropriate oversight to ensure that the data retention and destruction procedures are fully complied with in relation to equipment is critical to the integrity of and trust in *electoral* administration.

Ontario should implement the following when adopting *electronic poll books* and *vote tabulators* into their election delivery model:

7.3.1 Develop comprehensive procedures that set out how electoral data will be securely deleted from the equipment. These procedures must include a control check prior to providing *electronic poll book* or *vote tabulator* hardware to other Canadian *electoral management bodies.*

7.3.2 Ensure that all storage media of any/all *electronic poll books* and *vote tabulators* are completely and securely deleted, with no software or data relating to the electoral event remaining on the equipment, prior to the disposal, sale, or rental of the equipment.

7.3.3 This process should be confirmed by the *administrator* with the *electronic poll books* and *vote tabulator* vendors to ensure that it is sufficient to meet the requirements of the technology and equipment to which it is applied.

7.3.4 The *administrator* should implement dual confirmation (two-person control where both persons are of different ranks) that all data has been completely and securely deleted.

7.3.5 Ensure that if destruction of voting or *election* equipment is outsourced, the disposal vendor procedures are in accordance with Ontario GO-IT 25.0 *General Security Requirements* and Information Security and Privacy Classification Policy requirements and with any Elections Ontario procedures referenced above in section 7.3.1.

a. Require a certificate of destruction from the vendor stating that all data stored on the equipment has been properly erased and all hardware has been appropriately discarded.

7.4 Security and Integrity: Cyber Security

The use of *electronic poll books* and *vote tabulators* introduces risks when they operate on a network that depends on Wi-Fi and Internet connectivity. The *electronic poll book* allows the *election official* in *real-time* to add, review, and/or maintain *voter* register information and to identify and digitally strike-off of *voters'* names from the *voters' list* on a near *real-time* basis. Through this process, the *electronic poll book* participates in *real-time* data migration to transfer information to other systems supporting the electoral process.

Vendors are required under DGSI 119-1, *Election and Voting Technologies – Part 1: Vote Tabulators* (*Vote Tabulator* Product Standard) and DGSI 119-2, *Election and Voting Technologies – Part 2: Electronic Poll Books* (*Electronic Poll Book* Product Standard) to ship any technology being used for provincial *elections* in Ontario in a fully hardened state, with the option to enable functionality as required. Cyber security procedures specific to *electronic poll books* and *vote tabulators* should be developed within the organization's broader cyber security framework and cover activities related to the development, implementation, operation, and maintenance of technology solutions.

The Canadian Centre for Cyber Security (CCCS) provides guidance on cyber security considerations required to securely design, deploy, and operate *electronic poll books.* The CCCS security document covering *electronic poll books* (ITSM.10.101) outlines security configuration controls that Ontario should consider when evaluating, designing, or deploying *electronic poll books.*

The *Election Act* sets out a minimum restriction that applies only to the use of *vote tabulators.* Specifically, that the *vote tabulators* must not be part of or connected to an electronic network, except that it may be securely connected to a network after the polls close, for the purpose of transmitting information to the Chief Electoral Officer (S.4.5). As a result, many of the recommendations included below are not currently applicable to the use of *vote tabulators* but would become relevant if those who oversee provincial *elections* in Ontario decide to transmit results via remote transmission.

Ontario shall implement the following when adopting *electronic poll books* and *vote tabulators* into their *election* delivery model:

7.4.1 Develop security processes and procedures that meet or exceed the Government of Ontario security standards and guidelines as applicable, such as the GO-ITS 25.0 *General Security Requirements.*

7.4.2 Undertake a threat risk assessment to identify the likelihood that a cyber security event will occur based on assessments to determine where there are weaknesses that are prone to attack, and the potential resulting impacts. Carry out threat modeling based on threat-risk assessments to identify and map threats including, but not limited to, the following:

a. data integrity attacks;
b. cryptographic attacks;
c. wireless attacks;
d. distributed denial of service (DDoS);
e. malware attacks;
f. data breaches;
g. system attacks; and
h. supply chain attacks.

NOTE 1: Elections Ontario should determine the acceptable level of risk for achieving their organizational objectives and document risk tolerance decisions, cyber security requirements, and cyber security breaches, through the organization's public reporting mechanisms.

NOTE 2: Periodic audits by an independent third-party to verify that the *electoral management body* is following its security assessment and Incident Response Plans are an important component of transparency and ensuring trust in the integrity of *elections.*

7.4.3 Document decisions to enable or disable functions of the *electronic poll books* and *vote tabulators,* including risk management strategies as applicable.

7.4.4 Regularly update cyber security requirements based on the application of risk management processes to changes in business requirements and/or a changing threat and technology landscape.

7.4.5 Consistently and accurately monitor cyber security risks specific to *electronic poll books* and *vote tabulators* and ensure consideration of cyber security risks through all lines of operation in the organization.

7.4.6 Ensure that data, such as *voter* strike-off information, *ballot* images, and *cast vote* records, are encrypted at rest and during transmission.

7.4.7 Develop and implement procedures to address alleged and/or detected cyber security incidents, such as:

a. response processes and procedures are executed and maintained including those designed to contain, mitigate, and resolve incidents;

b. communication is clear, concise, correct, concrete, timely; and

c. analysis of response and support recovery activities.

NOTE: Integrity protection ensures that any inadvertent or intentional alterations to data are detected by the recipient.

7.4.8 Enable data communication interfaces or services that are required.

NOTE: Communication interfaces under DGSI 119-1, *Election and Voting Technologies – Part 1: Vote Tabulators* (*Vote Tabulator* Product Standard) and DGSI 119-2, *Election and Voting Technologies – Part 2: Electronic Poll Books* (*Electronic Poll Book* Product Standard) are required for the *electronic poll book, vote tabulators,* and peripheral devices. It is a requirement in the Product Standards that the manufacturer ship the product with these communication interfaces in a hardened state and that the *administrator* must choose to turn them on and to document associated risk acceptance. Communication interfaces, such as network and *USB* which are not being used for data transfer, should otherwise remain disabled.

7.4.9 Establish a single-purpose system to reduce the probable attack surface. Additional system functions such as general web browsing beyond the specific application, email services and others should be prevented on the devices.

7.4.10 Ensure data is encrypted in transit and at rest.

NOTE: Wireless networks (Wi-Fi) should be avoided on networks that are supposed to be isolated. Although these networks have nominal communications radii between 30 and 300 feet, devices with special antennas can listen to and interact with Wi-Fi over much longer distances, which can allow them to be attacked remotely.

7.4.11 Collaborate with security partners and where appropriate, provincial/federal agencies, other *electoral management bodies,* among other *election stakeholders* to develop a solution for supply chain management and cyber security for *elections,* including, but not limited to, transparency on corporate ownership structures, and corporate compliance with its own internal security policies and procedures, etc.

7.4.12 Work closely with the Government of Canada’s Computer Incident Response Team/Office of the Provincial Security Advisor, computer security companies, and Internet service providers to develop measures to check viruses, potential malware and systemic attacks, and develop response plans.

7.4.13 Take into consideration when developing the *electronic poll books,* the trade-off between network connectivity and security.

NOTE: Those who oversee provincial *elections* in Ontario shall use authorized networks that have continuous mutual two-way authentication mechanisms such as Virtual Private Networks (VPNs) to prevent known exploits and support updating to prevent any new vulnerabilities that are discovered. Those who oversee provincial *elections* in Ontario should build in adequate redundancies and system monitoring to identify when issues arise.

7.4.14 Ensure *election officials* and third parties are provided cyber security awareness education and are trained to perform their cyber security related responsibilities consistent with all related policies, procedures, and agreements.

7.5 System Access Control

Those who oversee provincial *elections* in Ontario must require that physical security measures be in place (see section 7.8) to ensure the integrity of all equipment and prevent *unauthorized access* during an *election.* This includes defining who has access to the equipment and ensuring that no individual can make unilateral modification to the equipment during an *election.*

Ontario shall implement the following when adopting *electronic poll books* and *vote tabulators* into their *election* delivery model:

7.5.1 Restrict access to physical and digital assets, and ensure approved associated facilities are limited to authorized users, processes, and devices.

7.5.2 Provide access only after formal *authorization* is granted, via unique identifiers and credentials, with formal records documenting the provision of access.

7.5.3 Develop and maintain policies and procedures relating to password protection that meet or exceed the password complexity outlined in the GO-ITS 25.0 *General Security Requirements.* Implement *multi-factor authentication,* based on a risk assessment, to mitigate *unauthorized access* and password attacks.

7.5.4 Develop formal procedures to protect against risks associated with obtaining files and software via external networks, or on any other medium, indicating what protective measures should be taken.

7.5.5 Implement system access *authorizations* to prevent malevolent activity with or without collusion.

7.5.6 Conduct regular software review for systems supporting critical business processes. The presence of unapproved files or *unauthorized* software should be formally investigated, documented, and reported.

7.6 Vote Tabulator Logic and Accuracy Testing

Verifiability of *vote tabulators* is critical for the trust in and integrity of the voting system. Tabulator *logic* and *accuracy (L&A) testing* is a set of activities that ensure that the *vote tabulators* and *assistive voting equipment* operate properly, and that the software has been programmed to accurately count or mark the "Electoral District Specific" *ballots* for a poll.

The *Election Act* requires *L&A testing* to be conducted before and after the election for the *vote tabulators* and for *assistive voting equipment* (S.44.1 & 45). *L&A testing* is also considered a best practice and can be found in existing documents such as the Election Assistance Commission (EAC) *Voluntary Voting Systems Guidelines 2.0* (VVSG 2.0).

Ontario shall implement the following when adopting *electronic poll books* and *vote tabulators* into their *election* delivery model:

7.6.1 Conduct *L&A testing* on each *vote tabulator,* and *assistive voting equipment,* both prior to the deployment to the field and post-*election.*

7.6.2 Ensure the *L&A test* includes a *test deck.*

NOTE 1: *L&A test decks* include *ballots* marked with pre-determined outcomes, such as;

a. the number of valid votes cast for each candidate (including those cast with *assistive voting equipment*);

b. *overvotes* or *undervotes;* and

c. all candidates received at least one valid vote.

NOTE 2: The number of valid votes cast per candidate should be randomly distributed to make the testing unpredictable.

NOTE 3: As per section 4.1.1.5 of DGSI 119-1, *Election and Voting Technologies – Part 1: Vote Tabulators* (*Vote Tabulator* Product Standard), the *electoral management* body will need to define what constitutes a mark (such as all marks darker than a fixed threshold that is marked in the *vote target* area).

7.6.3 Confirm and certify that an errorless *L&A test* was achieved, or the *vote tabulator,* and/or *assistive voting equipment,* shall not be deployed to a polling place.

7.6.4 Secure and retain all *election* documentation and equipment such as, pre-*election L&A test decks* and *ballots, results tape,* memory cards, etc. for post-*election L&A testing.*

7.6.5 Ensure all *L&A testing of the vote tabulator* is conducted with notice concerning the date, time, and location of the testing, and that invitations to observe *L&A testing* are extended to affected *stakeholders* such as candidates and *scrutineers.* Plain language documentation of the *L&A testing* should be provided to observers.

7.6.6 Maintain responsibility for conducting *L&A testing* and appoint a representative to oversee the conduct of *L&A testing.*

NOTE: A vendor representative should be on-site during *L&A testing* to provide technical expertise and support, as required. The vendor representative must not directly oversee, conduct, or intervene in the *L&A testing.*

7.6.7 Conduct a transparent results audit on the *vote tabulator,* if the post-event *L&A test* results are inconsistent with those generated by the pre-event *L&A test.*

NOTE: Protocols with respect to any failures in post-*election L&A testing* should be made public and provided to affected *stakeholders.*

7.7 Vote Tabulator Results Auditing

The *election* process and the result require meaningful verification of paper *ballots* cast and *tabulation* to ensure the *election* outcome reflects the valid votes cast. Result audits are performed to detect errors in the counting of *ballots* and to verify *election* results. There are several different kinds of results audits that those who oversee provincial *elections* in Ontario should consider adopting as a best practice, including *risk-limiting audits,* compliance audits, and *ballot*-level audits. In addition to confirming the *election* results and detecting tabulation errors, results auditing can deter hacking, malware, and fraud and help foster continuous improvement in *election* administration.

A *risk limiting audit* is a type of post-*election* audit that uses statistical methods combined with a manual review of paper *ballots* to confirm that the *vote tabulator* accurately generated the *election* results. Typically, a *risk limiting audit* is performed by manually comparing randomly selected batches of *ballots* to the *vote tabulator* totals for those *ballot* batches.

Ontario shall implement the following when adopting *electronic poll books* and *vote tabulators* into their *election* delivery model:

7.7.1 Develop auditing processes and procedures such as, *risk limiting audits* and *ballot* spot checks, to ensure that any tabulated results are correct. Included in these procedures is the need to identify actions to be taken if the results of the audit are different from those generated by the *vote tabulator.*

NOTE: The Ontario *Election Act* currently restricts the conduct of *risk-limiting audits,* as it requires that cast *ballots* are returned to the Chief Electoral Officer secured and sealed. These seals should only be opened if there is an order by a judge (S. 86). Within the current legislative framework, an alternative for Elections Ontario is to conduct a *vote tabulator* spot check which compares the *vote tabulator results tape* against *ballot* images from the *vote tabulator* memory cards. In this process, the *administrator* records the result for each *ballot* image to match the *vote tabulator results tape* for a particular poll against the *ballot* image and confirm the accuracy and integrity of the *vote tabulator* results.

7.7.2 Ensure the transparency of any auditing processes and procedures.

7.7.3 Conduct results audits in a timely fashion to facilitate a recount, ideally prior to the release of the official results.

7.7.4 Ensure that *election* information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

7.8 Physical Security/Control and Custody

In addition to ensuring the security and integrity of the technology as described above, it is essential to adopt practices that protect the physical security of the voting equipment, *ballots,* and other *election* supplies throughout the *election.* The *Election Act* sets out the custody and control of *ballot* paper, *ballot* boxes, used and unused *ballots,* and documents (S. 33, 74, 86).

The secure chain-of-custody specific to *ballots* incorporates multiple steps. These recommendations deal only with security requirements that relate specifically to *ballots* as they intersect with *vote tabulators* and not to the entire *ballot* chain-of-custody or broader *election* chain-of-custody issues. The remainder of the chain-of-custody is outside the scope of these standards and covered under the directives of the Chief Electoral Officer.

Ontario shall implement the following when adopting *electronic poll books* and *vote tabulators* into their *election* delivery model:

7.8.1 Develop processes and procedures for inventory management and chain-of-custody, such as for *vote tabulator* memory cards, *ballot* paper, and cast *ballots,* that are secure at all stages of the *election* and include the use of sign-off sheets, seal control sheets, and may involve conducting quality checks at relevant points in the *election* process.

7.8.2 Adopt tamper-evident indicators, such as asset tags, locks, and seals, in conjunction with use procedures supplied by producer(s).

7.8.3 Ensure there is a secure chain-of custody process in place for the deployment of *electronic poll books* to the returning office. This process may include affixing asset tags, sealing the asset into a case using tamper-evident indicators/seals, and testing that the software loaded onto each *electronic poll book* is working as intended.

7.8.4 Provide an asset control process such as a checklist for the returning office. The asset checklist may include matching asset numbers to ensure all appropriate equipment was received and ensuring that the proper software has been installed and is working as intended.

7.8.5 Develop guidelines and procedures for the *electronic poll books* and *vote tabulators* that identify and document functions, tasks, and responsibilities, relating to:

a. system maintenance; and

b. day-to-day operations.

Bibliography

[1] *Accessibility for Ontarians with Disabilities Act.*

[2] Canadian Centre for Cyber Security. (2021). *Cyber Threats to Canada's Democratic Process.* Government of Canada.

[3] Canadian Centre for Cyber Security (2012). *IT security risk management: A lifecycle approach (ITSG-33).* Government of Canada.

[4] Canadian Centre for Cyber Security (2012). *ITSG-33: Annex 1 – Departmental IT security risk management activities.*

[5] Canadian Centre for Cyber Security (2012). *ITSG-33: Annex 2 – Information system security risk management activities.*

[6] Canadian Centre for Cyber Security (2012). I*TSG-33: Annex 3A – Security control catalogue.*

[7] Canadian Centre for Cyber Security (2012). *ITSG-33: Annex 4A – Profile 1 & 3.*

[8] Canadian Centre for Cyber Security (2012). *ITSG-33: Annex 5 – Glossary.*

[9] Canadian Centre for Cyber Security. (2023). *Protecting Your Organization from Software Supply Chain Threats.* Government of Canada.

[10] Canadian Centre for Cyber Security (2022). *Security Considerations for Electronic Poll Books. Government of Canada.* Government of Canada.

[11] City of Toronto. (2022). *Use of Tabulators and Voter Assist Terminals.* City Clerk's Office – Toronto Elections.

[12] Connecticut Secretary of the State. *Connecticut Electronic Poll Book System Requirement Specification V1.0.* State of Connecticut.

[13] Council of Europe Committee of Ministers. (2017). *Recommendation CM/Rec (2017)5[1] of the Committee of Ministers to member States on standards for e-voting.*

[14] *Election Act* R.S.O. 1990, CHAPTER E.6.

[15] Elections Alberta, Office of the Chief Electoral Officer. (2017). *Procedure for the Use of Tabulators and Voter Assist Terminals at a By-election.* Elections Alberta.

[16] Elections Ontario, Office of the Chief Electoral Officer. (2022). *Directive for the 2022 General Election for the use of an alternative voting process.* Elections Ontario. https://www.elections.on.ca/directives.

[17] Elections Ontario, Office of the Chief Electoral Officer. (2022). *Directive for the 2022 General Election for Vote Counting Equipment and Accessible Voting Equipment.* Elections Ontario. https://www.elections.on.ca/directives.

[18] Elections Ontario, Office of the Chief Electoral Officer. (2023). Glossary. https://www.elections.on.ca/glossary.

[19] Essex, A., & Goodman, N. (2020). *Protecting Electoral Integrity in the Digital Age: Developing E-Voting Regulations in Canada. Election Law Journal: Rules, Politics, and Policy, 19(2), 1-18.* http://doi.org/10.1089/elj.2019.0568.

[20] Garnett, H. A., & James, T. S. (2020). *Cyber Elections in the Digital Age: Threats and Opportunities of Technology for Electoral Integrity. Election Law Journal: Rules, Politics, and Policy, vol. 19, no 2, p. 111-126.* http://doi.org/10.1089/elj.2020.0633.

[21] Garnett, H. A., & Pal, M. (2022). *Cyber Threats to Canadian Democracy.* McGill- Queen's University Press.

[22] Government of Ontario. (2016). *GO-ITS 25.0 General Security Requirements.* https://www.ontario.ca/page/go-its-250-general-security-requirements.

[23] Indiana Secretary of State. (2018). *Assessment of Learning of Indiana Election Personnel on Electronic Poll Books: Guidelines by Voting System Technical Oversight Program.*

[24] Indiana Secretary of State. (2022). *Indiana Electronic Poll Certification Test Protocol.* Bowen Center for Public Affairs.

[25] International Institute for Democracy and Electoral Assistance. (2011, December). *Introducing Electronic Voting: Essential Considerations.* Policy Paper. Available at: https://www.idea.int/es/publications/catalogue/introducing-electronic-voting-essentialconsiderations.

[26] International Organization for Standardization. (2023). *Financial services — Biometrics — Security framework* (ISO Standard Nº. ISO 19092:2023). www.iso.org/standard/78308.html.

[27] International Organization for Standardization. (2022). *Information technology, Security techniques – Code of practice for information security controls* (ISO Standard Nº. SO/IEC 27002:2022). https://www.iso.org/standard/75652.html.

[28] International Organization for Standardization. (2021). *Information Technology – Storage management – Part 2: Common Architecture* (ISO Standard Nº ISO/IEC 24775-2:2021). https://www.iso.org/obp/ui/en/#iso:std:iso-iec:24775:-2:ed-2:v1:en.

[29] International Organization for Standardization. (2019). *Quality management systems — Particular requirements for the application of ISO 9001:2015 for electoral organizations at all levels of government* (ISO Standard Nº. 54001:2019). https://www.iso.org/standard/75288.html.

[30] International Foundation for Electoral Systems. (2023). *Electoral Cybersecurity Briefing Series.* https://www.ifes.org/publications/electoral-cybersecurity-briefing-series.

[31] Michigan Department of State Bureau of Elections. (2019). *Test Procedure Manual for Tabulators and Voter Assist Terminals*. State of Michigan.

[32] New Jersey Division of Elections. (2021). *Electronic Poll Book Regulations.* National Institute of Standards and Technology. Election Terminology Glossary. (2023) Available at: https://csrc.nist.gov/glossary.

[33] Organization for Security and Co-operation in Europe. (2013). *Handbook for the Observation of New Voting Technologies.* Available at: https://www.osce.org/odihr/elections/new_voting_technologies.

[34] Pratama, H., & Salabi, N. (2020). *Adoption of Voting Technology: A Guide for Electoral Stakeholders in Indonesia. International Institute for Democracy and Electoral Assistance.* Available at: https://www.idea.int/sites/default/files/publications/adoption-of-voting-technology.pdf.

[35] Ross, R., Winstead, M., & McEvilley. (2022) *Engineering Trustworthy Secure Systems: NIST Special Publication NIST SP 800-160v1r1.* Available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1r1.pdf.

[36] Schwartz, B., & Grice, D. (2013). *Establishing a Legal Framework for E-Voting in Canada.* Elections Canada.

[37] State of Indiana. (2013). *Certification Test Report for Examination of Electronic Poll Book for the Voting System Technical Oversight Program.*

[38] Texas Secretary of State. (2019). *Texas Certification Procedures for Electronic Pollbooks.*

[39] U.S. Election Assistance Commission. (n.d.). *E-Pollbook Certification Procedures & System Requirements.*

[40] U.S. Election Assistance Commission. (2021). *Voluntary Voting System Guidelines Version 2.0.*

[41] Walker, J., Bajaj, N., Crimmins, B.L., Halderman, J.A. (2022). *Logic and Accuracy Testing: A Fifty-State Review.* In: Krimmer, R., Volkamer, M., Duenas-Cid, D., Rønne, P., Germann, M. (eds) Electronic Voting. E-Vote-ID 2022. Lecture Notes in Computer Science, vol 13553. Springer, Cham. https://doi.org/10.1007/978-3-031-15911-4_10.

Appendix 1: Advisory Committee on Standards for Voting Technologies Membership

Appointed by:	Advisory Committee Member
Chief Electoral Officer	1. Jean-Pierre Kingsley (Chair) 2. Dr. Nicole Goodman 3. Dr. Mkabi Walcott
Progressive Conservative Party of Ontario	4. Michael Crase 5. Dan Duncan
New Democratic Party of Ontario	6. Karla Webber-Gallagher 7. Donald Eady
Ontario Liberal Party	8. Milton Chan 9. Christine McMillan
Green Party of Ontario	10. Craig Cantin

Appendix 2: Advisory Committee on Standards for Voting Technologies Principles

Note: These principles were developed to guide the development of Standards and are not intended to be read as part of the Standards.

Democratic Election Principles:

I. **Accessibility**

   i. The election shall be accessible and consistent for all electors.

   ii. The election shall provide accessibility of the vote to all electors, including through accessible voting equipment and other election technology.

   iii. The election shall be inclusive of all electors, including through the deployment of voting equipment and other election technology.

II. **Equality of the vote**

   i. All voters shall exercise their right to vote without influence or being prevented from participating in the voting process.

   ii. One vote per voter.

   iii. The election process shall avoid duplication of voters' data.

   iv. The election process shall authenticate each voter prior to issuing a ballot.

   v. All voters shall receive the correct information about the election and voting process in time to exercise their right to vote.

   vi. Elections shall be compliant with the democratic rights of citizens set out in the *Canadian Charter of Rights and Freedoms.*

   vii. All voters shall have equal opportunity to take part in the vote.

III. **Ballot Secrecy**

   i. The election process must protect the secrecy of the ballot.

   ii. The election process shall not contain nor produce information and records that can match a ballot to a given voter to ensure that all votes are cast anonymously.

   iii. Voters shall not be able to show proof of how they voted to anyone.

IV. **Privacy**

   i. All voters shall exercise their right to vote privately and independently.

   ii. Electors' personal information shall be gathered and used only for electoral purposes as authorized under the Ontario *Election Act.*

   iii. Electors' personal information shall be protected in all formats, including digital.

V. Transparency

i. The election shall be conducted in a manner that is open, simple to understand, verifiable and accountable to electors, candidates, political parties, scrutineers, and other individuals as permitted under the Ontario *Election Act.*

ii. Candidates, political parties, scrutineers, and other individuals as permitted under the Ontario *Election Act* shall have the opportunity to meaningfully observe, monitor and scrutinize the election.

iii. The election administration body shall be accountable to electors through the legislature for the conduct of the election as directed under the Ontario *Election Act.*

VI. Integrity

i. The election process and the results shall maintain the integrity of the election and the democratic rights of all electors.

ii. The election process and the results shall be verifiable. The election results shall accurately reflect the valid votes cast.

iii. The election process and the results shall be free from any unauthorized access, manipulation, fraud, or error.

iv. The election shall be operated in a manner that demonstrates trustworthiness and confidence in the process.

v. The election process shall be fair and non-biased and shall treat candidates and voters fairly and consistently.

VII. Verifiability

i. The election process and the result shall allow for meaningful verification of paper ballots cast and tabulation to ensure the election outcome reflects the valid votes cast.

ii. The voter shall be able to verify that the ballot they have marked is accurate.

iii. The results of the election shall allow for timely audits and permit the possibility of recount to determine the results of the election.

iv. The voting process must allow for meaningful and timely scrutiny and the ability to verify the accuracy and correctness of the voting process and the election results by candidates, political parties, scrutineers, and other individuals as permitted under the Ontario *Election Act.*

v. Election results reporting shall be meaningfully detailed and contain a manageable number of electors for the purposes allowed under the Ontario *Election Act* by candidates, political parties, and other authorized entities.

VIII. Security

i. The election shall ensure the reliability and security of the voting process and results.

ii. The election process shall have mechanisms to detect problems and prevent or detect tampering with the vote.

iii. The election process shall ensure the protection of data and stored information, as required under Ontario privacy legislation.

Technical Design Principles: Voting Technologies

I. Voting Technology Design

i. The voting technology is designed to carry out the election process accurately and securely.

ii. The voting technology is designed to align with election process procedures and regulations as set out in the Ontario *Election Act.*

iii. The voting technology is designed in a user-friendly manner that is accessible to all voters.

iv. The voting technology is designed to provide transparency and accountability.

v. The voting technology is designed to be operationally implementable.

vi. The voting technology is designed with materials that meet the requirements of a supply chain risk management framework.

vii. The design and implementation of technology in the facilitation of the election must maintain or improve the level of transparency; political entities' ability to scrutinize electoral proceedings; levels of detail of reporting; meaningful reporting of results; the public's ability to review and analyse the results and must uphold the Democratic Election Principles.

II. Simplicity and Ease of Use

i. The voting technology design and functions can be easily interpreted and understood.

ii. The voting technology can be used accurately.

iii. Voters, political parties, candidate representatives, scrutineers, and election staff can understand and interpret information, including instructions, messages from the system, and error messages.

III. Interoperability

i. The voting technology is designed to support interoperability in its interfaces to external systems, its interfaces to internal components, its data, and its peripherals.

ii. The voting technology data is in an interoperable format.

iii. The voting technology uses widely used hardware interfaces, formats, and communications protocols.

IV. Verifiability

i. The voting technology allows for paper ballots to be marked, verifiable, and cast as intended.

ii. The source and integrity of electronic tabulation reports are verifiable.

V. Auditability

i. The voting technology shall be auditable.

ii. The voting technology software can be tested and verified by election staff, witnessed, or observed by party and candidate representatives at each machine before a vote is cast.

iii. The voting technology records are resilient in the presence of intentional forms of tampering and accidental errors.

iv. Both physical and digital aspects of the voting technology are available for inspection and testing.

v. The voting technology shall report any irregularities or errors that were identified.

VI. **System integrity**

i. The voting technology shall protect the integrity and confidentiality of sensitive data.

ii. The voting technology maintains the integrity of software, firmware, and other critical components.

iii. The voting technology shall support mechanisms to detect and prevent any unauthorized access or tampering.

iv. The voting technology authenticates administrative users before granting access to functions and restricts its services to unauthorized entities.

Technical Design Principles: Election Technologies

I. **Election Technology Design**

i. The election technology is designed to carry out the election process accurately and securely.

ii. The election technology is designed to align with election process procedures and regulations as set out in the Ontario *Election Act.*

iii. The election technology is designed in a user-friendly manner that is accessible to all electors.

iv. The election technology is designed to provide transparency and accountability.

v. The election technology is designed to be operationally implementable.

vi. The election is designed with materials that meet the requirements of a supply chain risk management framework.

vii. The design and implementation of technology in the facilitation of the election must maintain or improve the level of transparency; political entities' ability to scrutinize electoral proceedings; levels of detail of reporting; meaningful reporting of results; the public's ability to review and analyse the results and must uphold the Democratic Election Principles.

II. **Simplicity and Ease of Use**

i. The election technology design and functions can be easily interpreted and understood.

ii. The election technology can be used accurately.

iii. Voters, political parties, candidate representatives, scrutineers, and election staff can understand and interpret information, including instructions, messages from the system, and error messages.

III. **Interoperability**

i. The election technology is designed to support interoperability in its interfaces to external systems, its interfaces to internal components, its data, and its peripherals.

ii. The election technology data is in an interoperable format.

iii. The election technology uses widely used hardware interfaces, formats, and communications protocols.

IV. **Access Control**

i. The election technology implements mechanisms to authenticate users and prevent unauthorized changes and manipulation.

ii. The election technology shall be configured in such a manner that the infrastructure is able to authenticate each user prior to access.

iii. The election technology shall be configured to ensure two-factor authentication is employed to access the device.

iv. The election technology authenticates users before granting access to functions and restricts its services to unauthorized entities.

V. **Authentication**

i. The election technology shall allow for the authentication of each voter prior to issuing a ballot.

ii. The election technology shall allow election staff to enter information regarding a voter who has appeared to vote to verify whether the voter is eligible to vote, and if so, whether the voter has already cast a ballot at the election or returned a special ballot.

VI. **Auditability**

i. The election technology shall be auditable.

ii. The election technology records are resilient in the presence of intentional forms of tampering and accidental errors.

iii. Both physical and digital aspects of the election technology are available for inspection and testing.

iv. The election technology shall report any irregularities or errors that were identified.

VII. **System Integrity**

i. The election technology shall protect the integrity and confidentiality of sensitive data, as required by privacy legislation in Ontario.

ii. The election technology maintains the integrity of software, firmware, and other critical components.

iii. The election technology shall support mechanisms to detect and prevent any unauthorized access or tampering.

iv. The election technology shall protect electors' personal information in all digital formats.

v. The election technology must allow for meaningful testing and risk management evaluations.

VIII. **Reliability**

i. The election technology shall be reliable and available for use when needed.

ii. The election technology shall be functional and shall have preestablished system failure solutions and channels readily available, including solutions that do not rely on active connections.

Appendix 3: Conformance Language

Standards use specific keywords such as “shall” and “should” or “must” and “may” which are common in requirements and recommendations for the proper implementation of the standards subject matter. The use of these terms by the International Standards Organization in its *Quality Management Systems – Requirements* (ISO 9001:2015) and by the U.S. Election Assistance Commission in its *Voluntary Voting System Guidelines* (VVSG) are used to differentiate mandatory requirements and advisory recommendations, respectively. The use of the term “shall” indicates the requirements that must be adhered to for compliance with those Standards.

In the context of these *Recommendations for Management Standards on Electronic Poll Books and Vote Tabulators,* the “shall” statements are essential for ensuring the integrity, security, and reliability of the *vote tabulators* and *electronic poll books* used in the delivery of *elections.* Compliance with these requirements is necessary to maintain a trustworthy and accurate voting process.

“Should” statements are used for non-critical or recommended practices, such as system performance, or suggestions for certain optional features that can enhance the voting experience but are not mandatory for standards compliance.

#	ISO/TS 54001:2019(E) Quality management systems — Particular requirements for the application of ISO	Voluntary Voting System Guidelines VVSG 2.0
1.	**“Shall”** indicates a requirement	**“Must”** indicates a mandatory requirement, synonymous with “is required to”
2.	**“Should”** indicates a recommendation	N/A
3.	N/A	**“Must not”** also indicates a mandatory requirement, but the requirement is to not do something
4.	**“May”** indicates a permission	**“May”** indicates an optional, permissible action and often suggests one possible way of conforming to a more general requirement
5.	**“Can”** indicates a possibility or a capability	N/A

Appendix 4: Standards Referenced in the Management Standard

Standard / Document ID Reference	Standard Full Name	Brief Description of the Standard	Reference Link
DGSI 119-1	*Election and Voting Technologies – Part 1: Vote Tabulators*	This Standard, DGSI 119-1 specifies the minimum requirements for the design, installation, operation, and maintenance of vote tabulators and vote tabulator systems.	–
DGSI 119-2	*Election and Voting Technologies – Part 2: Electronic Poll Books*	This Standard, DGSI 119-2 specifies the minimum requirements for the design, installation, operation, and maintenance of electronic poll books, and electronic poll book configurations.	–
GO-ITS 25.0	*General Security Requirements*	The GO-ITS 25.0 General Security Requirements defines general security requirements for the protection of the integrity, confidentiality, and availability of Government of Ontario networks and computer systems.	https://www.ontario.ca/page/go-its-250-general-security-requirements
N/A	*Elections Ontario Identification Policy*	This policy sets out what kinds of documents can serve as a person's proof of identity (also known as "proof of name") and a person's proof of place of residence ("proof of residence" for short).	–
N/A	*Elections Ontario Integrated Accessibility Standards Policy*	This policy addresses the mandatory requirements and standards under Ontario's Integrated Accessibility Standards Regulation (IASR) which establishes accessibility standards for information and communications, employment, transportation, design of public spaces and customer service.	https://www.elections.on.ca/content/dam/NGW/sitecontent/2017/resources/policies/Integrated%20Accessibility%20Standards%20Policy.pdf
ISO 31000:2018	*Risk Management – A Practical Guide*	ISO 31000:2018 provides guidelines on managing risk faced by organizations. The application of these guidelines can be customized to any organization and its context.	https://www.iso.org/standard/65694.html

Standard / Document ID Reference	Standard Full Name	Brief Description of the Standard	Reference Link
ISO 9001:2015	*Quality management systems*	Guidance for implementing quality assurance and continuous improvement.	https://www.iso.org/standard/62085.html
ITSG-33	*IT security risk management: A lifecycle approach*	The Government of Canada's cyber security reference manual. Guidance document regarding IT security risk management activities that should be undertaken to manage risks associated with an IT system throughout its lifecycle.	https://www.cyber.gc.ca/en/guidance/it-security-risk-management-lifecycle-approach-itsg-33
VVSG 2.0	*Voluntary Voting Systems Guidelines 2.0 (VVSG 2.0)*	Developed by the Electoral Assistance Commission (USA), the Voluntary Voting System Guidelines (VVSG) are a set of specifications and requirements against which voting systems can be tested for certification.	https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines