CAN/DGSI 111-1:2024
NATIONAL STANDARD OF CANADA

First Edition
2024-12

Online Voting – Part 1: Implementation of Online Voting in Canadian Municipal Elections

35.020

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

- Page left intentionally blank -

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

Table of Contents

Introduction vi

Context 1

1 Scope 2

2 Normative references 3

3 Terms and definitions 4

4 Security of systems and data 6

4.1 Online voting security 6

4.2 Voter Security 11

4.3 Online voting provider security 11

5 Voter identity and vote authentication 11

5.1 Voter identity 11

5.2 Vote authentication 12

6 Testing and auditability 12

6.1 Testing 12

6.2 Auditability 13

6.3 Documentation 13

7 Access to online voting services and voter election information 14

7.1 Access, encryption, retention, and transfer of information 14

8 Secrecy of vote 16

8.1 Maintaining privacy, anonymity, integrity, and secrecy 16

9 Ballot design and accessibility 17

9.1 Useability and accessibility requirements 17

10 Bandwidth and network capacity 18

10.1 Technical network requirements and outages 18

11 Election Management/Administration 19

11.1 Staffing and personnel 19

11.2 Risk assessment and security 19

Bibliography 21

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

- Page left intentionally blank -

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

Foreword

The Digital Governance Standards Institute (DGSI) develops digital technology governance standards fit for global use. The Institute works with experts, as well as national and global partners and the public to develop national standards that reduce risk to Canadians and Canadian organizations adopting and using innovative digital technologies in today's digital economy.

DGSI standards are developed in accordance with the *Requirements & Guidance – Accreditation of Standards Development Organizations*, 2019-06-13, established by the Standards Council of Canada (SCC).

Attention is drawn to the possibility that some of the elements of this Standard may be the subject of patent rights. DGSI shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of this Standard are included in the Introduction.

For further information about DGSI, please contact:

Digital Governance Standards Institute
500-1000 Innovation Dr.
Ottawa, ON K2K 3E7
www.dgc-cgn.org

A National Standard of Canada is a standard developed by a Standards Council of Canada (SCC) accredited Standards Development Organization, in compliance with requirements and guidance set out by SCC. More information on National Standards of Canada can be found at www.scc.ca.

SCC is a Crown corporation within the portfolio of Innovation, Science and Economic Development (ISED) Canada. With the goal of enhancing Canada's economic competitiveness and social well-being, SCC leads and facilitates the development and use of national and international standards. SCC also coordinates Canadian participation in standards development, and identifies strategies to advance Canadian standardization efforts.

Accreditation services are provided by SCC to various customers, including product certifiers, testing laboratories, and standards development organizations. A list of SCC programs and accredited bodies is publicly available at www.scc.ca.

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

- Page left intentionally blank -

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

Introduction

This is the First Edition of CAN/DGSI 111-1:2024, Online Electoral Voting – Part 1: Implementation of Online Voting in Canadian Municipal Elections.

CAN/DGSI 111-1:2024 was prepared by the Digital Governance Standards Institute Technical Committee 11 (TC 11) Online Electoral Voting for elections, *referendums*, and other types of municipal votes, comprised of more than 100 thought leaders and experts in cybersecurity, political science, public policy, election administration and related subjects. This Standard was approved by a Technical Committee formed balloting group, comprised of 3 producers, 4 government / regulator / policymakers, 1 user, and 3 general interests.

All units of measurement expressed in this Standard are in SI units using the International System of Units (SI).

This Standard is subject to technical committee review beginning no later than one year from the date of publication. The completion of the review may result in a new edition, revision, reaffirmation or withdrawal of the Standard.

The intended primary application of this Standard is stated in its scope. It is important to note that it remains the responsibility of the organization adopting the Standard to judge its suitability for a particular application. This Standard is intended to be technology agnostic.

This Standard is intended for, but is not limited to, conformity assessment.

ICS 35.020

CETTE NORME NATIONALE DU CANADA EST DISPONIBLE EN VERSIONS FRANÇAISE ET ANGLAISE

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

- Page left intentionally blank -

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

Context

The use of online voting in the municipal elections of select Canadian provinces has been occurring since 2003 and is continually expanding. Currently, *online voting service*s are implemented to either (1) supplement traditional paper-based voting services or (2) as a replacement for them. A growing number of municipalities are opting for fully digital elections (and to remove paper *ballots*) (Cardillo et al., 2019). In cases where elections are fully digital, municipalities either use online voting only or a combination of online and telephone *ballots*.

Municipalities have moved towards online voting to encourage turnout, enhance *voters'* convenience and accessibility, and to realize administrative efficiencies such as generating faster results and reducing *ballot* errors (Goodman and Pyman, 2016; Goodman and Spicer, 2019). In particular, online voting has been found to improve accessibility for marginalized or absentee *voter*s and to decrease barriers associated with voting (Budd et al., 2019; Goodman et al., 2010).

It is important that *online voting service*s be designed to deliver assurance and transparency and implemented with a standardized approach to both promote and maintain public trust. It is also important that formal partnerships and collaborative frameworks be established between technology companies and academic researchers and institutions to foster innovation and continuous improvement of online voting technologies and methodologies and to ensure that the evolution of the standard corresponds with technological advancements and empirical research findings. Further guidance and leadership will also be needed from Canada's federal and provincial governments to facilitate the implementation and continued development of the standard in alignment with its underlying principles.

This standard was developed as a means of promoting continuous improvement in providing *online voting services* to citizens. The history of *online voting* use across jurisdictions has shown us that incremental change is best and leads to greater success.

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

Online Electoral Voting – Part 1: Implementation of Online Voting in Canadian Municipal Elections

1 Scope

This standard specifies (1) technical design requirements for *online voting service*s and (2) best practices for *election administrators* who are implementing online voting in Canadian municipal elections. These are separated into two sections in the standard.

While there are types of telephone voting that use an internet connection, any type or form of telephone voting would be subject to a different standard given unique difference in design and implementation.

Considerations are given to:

1. Thresholds to measure the security of *online voting service*s, including the security and privacy of voting data both in transit and in storage across the *devices* and entities involved in the election (including *voter*s, *online voting providers*, independent 3rd parties, *scrutineers*, *election administrators* and staff).

2. Documentation and processes for *voter* identity and authentication.

3. Documentation and processes for *formal verification* requirements, including evidence of correctness (e.g., independently verifiable evidence supporting the outcome of the election).

4. Minimum requirements for personnel (e.g., staffing) and the provisioning of network and computational resources and capacity.

5. *Logic and accuracy testing*, discovery, documentation and processes of the testing and auditability of systems, including clear parameters regarding when they *shall* be audited and by whom, and how much detail of the system *should* be made public.

6. Documentation and processes regarding access to the *online voting service*, *voter information/data* and election information. This includes parameters that define who has administrator/privileged access to different parts of the system (e.g., *election administrators*, *election officials*, and the *online voting provider*) and control over making system changes as well as defining the role of the *online voting provider* and their level of access to *voter information/data* and vote information.

7. Protocols and processes to protect the secrecy of the vote to ensure that no one (including system operators and *election officials*) can trace vote choices back to identifiable individual *voter*s, defining who has privileged access to what information and what technical privacy guarantees are required.

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

8. Documentation and processes surrounding *ballot* design, including measures for ensuring that *ballots* display consistently across operating systems, *devices*, browsers, and the *ballot* displays all required options, including all qualified *candidate* names and options (e.g., spoiling, declining, none of the above) as required by law.

9. Documentation, protocols, and processes for observing and auditing the electoral process implemented through the *online voting service*.

10. Clear and defined documentation of accessibility requirements to ensure that all *voter*s can successfully cast a *ballot* on the *online voting service*.

11. Establishing procedures to clarify the role of *candidates* and *scrutineers,* including when and how the *online voting service* is demonstrated to them and their role in the tabulation and *verification* of results. As part of the *online voting service*, the practice of *scrutineering shall* have meaning and soundness.

12. Technical design and documentation requirements so that *online voting provider*s are transparent and clear about their product design and whether their product conforms to the relevant and applicable provisions within this Standard. *Online voting provider*s *should* disclose their compliance or identify areas of non-compliance when bidding on contracts to provide *online voting service*s for municipal elections.

How to use this document

Municipalities and their *election administrators* can use this document to assess their *online voting provider*s. Likewise, they can use it to inform requests for proposals from *online voting provider*s if they are considering implementing an *online voting service* in their elections. It can also be used by *election administrators* to guide them in the development of policies and procedures related to the deployment of online voting.

Smaller-sized municipalities may lack the resources to contract customized online voting solutions, so this Standard aims to outline the minimum technical requirements for *online voting provider*s to ensure there is a baseline for the use of this technology in the Canadian market, specifically in local elections.

*Online voting provider*s *should* use this document to assess their current practices and service levels being provided to municipalities in Canada. Ideally, *online voting provider*s *should* complete a cyber security risk assessment (e.g., in accordance with the CyberSecure Canada Program) prior to offering an *online voting service* to the Canadian municipal market to determine their overall threat risk level.

2 Normative references

There are no normative references in this document.

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

3 Terms and definitions

For the purposes of this document, the following words, terms, and definitions *shall* apply:

ballot
An image on an internet-enabled *device* of a *ballot* for an election to be voted for, including all choices available to the *voter*s, and containing spaces in which the *voter*s mark their selections.

candidate
Person who competes for public office in a municipal election (in this context).

[SOURCE: ISO/TS 54001:2019, 3.2.1]

cast
The action a *voter* takes in confirming their choices and submitting their selections via the *online voting service*.

cast vote record
An electronic record of the *voter*'s *ballot* selections, produced by the *online voting service*, providing a record of *voter* selections that can be counted efficiently to produce *election results* that are independently auditable.

coordinated vulnerability disclosure
A process for disclosing newly discovered vulnerabilities in hardware and software directly to the online voting providers of the affected product. It provides the online voting provider with the opportunity to implement and deploy a mitigation in advance of public disclosure.

device
A piece of electronic equipment that interacts with the physical world and has at least one network interface, that the user operates to cast their *ballot*.

election
A formal process in which *voter*s select *candidates* to be elected to one, or more, offices; for the purposes of this document, can also include the process by which *voter*s select options in response to a referendum or *ballot* question.

election administrator
The individual with ultimate responsibility for the delivery and control of the election within the jurisdiction to which they are appointed.

NOTE: In the Canadian municipal context, this can refer to the Assistant Municipal Electoral Officer(s), Chief Administrative Officer, Chief Election Officer, Chief Electoral Officer, Chief Municipal Electoral Officer, Clerk, Deputy Chief Election Officer(s), Deputy Chief Municipal Electoral Officer, Deputy Returning Officer, Election Clerk, Election Commissioner, Municipal Elections Officer, Municipal Electoral Officer, Registrar, Returning Officer(s), Secretary-Treasurer, Senior Administrative Officer, or Senior *Election Official*. It varies both between provinces and territories, across municipalities and within a single province or territory.

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

election official
A person appointed by the *election administrator* in accordance with the local election laws to fulfill certain duties as the *election administrator* deems necessary.

election results/statement of vote
Output of the *online voting service* for each *election* that provides the *election results* in an interoperable format for final tabulation of *election results*.

eligible
For the purpose of this document, a *voter*'s eligibility pertains to whether they have been issued credentials to access and vote using the online voting system. The legal requirements pertaining to the eligibility of an individual to vote in the *election* is outside the scope of this definition.

formal verification
Testing the functionality of software. This includes proving or disproving the correctness of software with respect to a formal specification or a property, using formal mathematical methods.

[SOURCE: ISO/IEC 23643:2020, 3.10]

independent 3rd party
Any organization or individual involved in the development, deployment, and/or providing support to the *online voting service* that is not the direct *online voting provider*.

keyholder
Individual who is a part of the body responsible for the generation of the encryption key.

logic and accuracy (L&A) testing
Equipment and system readiness tests whose purpose is to detect bugs, malfunctioning *devices* and improper *election*-specific setup before the equipment or systems are used in an *election*.

municipality
The local jurisdiction which is using, or could use, a form of online voting to collect or count votes in a municipal *election*, or referendum, or other type of vote.

online voting provider
The voting provider of the *online voting service*.

online voting service
An *online voting service* where *ballots* are completed, cast, transmitted, received, and counted over an electronic communications network.

patched
Has had all known flaws remediated.

plebiscites/ referendums
A direct vote open to all members of the electorate on a specific issue, law or proposal.

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

scrutineer
An individual, or group of individuals, appointed as a *scrutineer* in accordance with the applicable legislation to observe the voting process.

service level agreement (SLA)
An agreement between a service provider and a customer.

shall
A requirement.

should
A recommendation.

verification
In the context of electoral technology, a confirmatory mechanism that produces robust evidence that votes in an *election* were not tampered with and the counting of votes is correct.

vote counting
Process of taking account of votes cast by the electorate to determine the final results of an *election*.

(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)

voter
A person who is entitled to cast a *ballot* in an *election*.

voter information/data
Personal information on *voter*s, including *ballot* sections and *cast vote record* (CVR).

voting period
The time during which *voter*s may access and cast *ballots* using the *online voting service* provided in an *election*, which includes both the advance *voting period* and voting day.

4 Security of systems and data

4.1 Online voting security

4.1.1 The *online voting provider shall* provide documentation to the *municipality* on how they will detect and prevent or adequately mitigate each of the commonly cited classes of risks:

a. External threat actors – one or more individuals seeking to gain access to systems or parts thereof, to compromise the confidentiality, integrity, availability, and/or providence of the *election* process and related data.

NOTE: This includes all unauthorized attempts to gain access to any component of the *online voting service* architecture including the *voter*-client access, municipal

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

administrative access, or server-end systems. It is assumed that external threat actors are not employed by either *municipality* or *online voting provider*.

b. Insider threats – individuals working within/for the *municipality* and/or the *online voting provider*s with privileged virtual and/or physical user access, seeking to compromise the confidentiality, integrity, availability, and/or providence of the *election* process and related data.

   NOTE: This may include attempts to observe voting choices, change the cast votes, and/or illegitimately prevent votes from being cast. Actors within this category include not only *online voting provider*(s) and *municipality*(ies) but also any *independent 3rd party* subcontractors including cloud providers, colocation providers, printing providers etc.

c. Malware – software that undetectably observes, modifies, or denies a *voter*'s vote.

d. Denial of Service (DoS) or Distributed Denial of Services (DDoS) – an attack on the *online voting service* that renders the solution inaccessible or unavailable for some, or all, *voter*s.

e. Social engineering – a deceptive technique where the attacker sends a fraudulent message designed to trick a person into revealing confidential, personal, or sensitive information in order to deploy malicious software on the victim's infrastructure and disrupt the *election*.

f. *Voter*'s *device* tampering – malicious actors using a compromised online voting interface (which could include an application, browser application, or operating system) to affect the functionality of the voting application, including end-user access of a deceptive application.

g. Insufficient IT resources – all *online voting provider*s and third-party service providers *shall* ensure sufficient IT staff and resources including bandwidth capacity that may be needed for testing, regular monitoring and detection; proper capacity for timely cyber incident response; and project management.

h. Weak authentication procedure – possibility for *voter* and/or *election administrator* impersonation.

   NOTE: The *online voting provider should* adequately explain the authentication procedures and suggest a strong authentication process, understanding that the responsibility for authentication ultimately falls on the *municipality*.

i. *Voter* data/information penetration, exfiltration, and eavesdropping including but not limited to:

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

- Server-side eavesdropping by system administrators working for the *online voting service provider*;
- *Voter* or *municipality*-side exfiltration of *voter information/data* by malware;
- Server-side exfiltration of *voter information/data* by malware;
- Server penetration and modification of *voter information/data* by external hackers;
- Unauthorized server-side *voter information/data* modification by privileged administrators;
- Server penetration and exfiltration of *voter information/data* by remote hackers;
- Insider threats;
- *Voter* coercion.

j. Server-side logic and accuracy errors.

k. Server-side network security configuration errors which would increase the vulnerability of the network and/or system.

l. Unauthorized modification of voting system code, i.e. server-side code being different from what was scrutinized.

4.1.2 The *online voting provider shall* provide a list of security controls and/or guarantees and a summary of security protocols and processes that are regularly employed to protect the vote, including any information that is received and transmitted as part of this process prior to the start of the *voting period*, as well as periodically throughout the *voting period* (as mutually agreed upon with the *election administrator*) and after the *voting period* ends.

4.1.3 When applicable, the *online voting provider should* maintain direct control of the systems' equipment, which may include direct physical custody, while running the *online voting service*. Details about technical infrastructure supporting the *online voting service shall* be provided to municipalities, including the location where the data is stored. The *online voting provider shall* likewise be responsible for all sub-contracted third-party services.

4.1.4 The *online voting provider should* deliver the systems without any user data (i.e., in a *patched* and 'sanitized' state).

4.1.5 Development *shall* be done with oversight and/or within teams of more than one individual (including software development, hardware deployment, user testing, document management, systems configuration, operational maintenance, etc.).

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

4.1.6 When practicable, the system *should* be deployed into heterogeneous environments to mitigate against single points of compromise (e.g. in different physical locations, with different power providers, through different network providers, different operators, using different equipment types, etc.).

4.1.7 The *online voting provider shall* not store or deploy any *election* data, code, or software of the contest in production where the actual votes will be cast, on servers and/or infrastructure located outside of Canada, including any centralized data centers or *election* infrastructure used in cloud-based environments.

4.1.8 All data *should* be end-to-end encrypted both in transit and at rest. Measures *should* be taken to guarantee the long-term confidentiality and integrity of encrypted data, for example, through its secure erasure after the contest.

4.1.9 The *online voting service shall* include redundant firewalls, intrusion detection systems/ intrusion prevention systems, verbose access logging with periodic backup, threat detection and prevention.

4.1.10 The *online voting provider shall* adopt business continuity and data recovery plans that ensure the lowest Recovery Time Objective (RTO) at 1 hour and Recovery Point Objective (RPO) at 15 minutes.

4.1.11 All *election* staff (including sub-contractors) *shall* work on secured *devices* (encrypted and strong passphrase protected and networks) throughout the *voting period*. The *devices* used by *election* staff *shall* also be secured by multi-factor authentication.

NOTE: Strong methods of authentication *should* be used (i.e. an authenticator app or security token) for administrators. Email and SMS based authentication is a weaker option and *should* be avoided when possible. For further guidance, refer to Canadian Centre for Cyber Security guidelines on best practices for passphrases and passwords (ITSAP.30.032).

4.1.12 Any administrative processes, procedures, or functions provided by the *online voting provider* for use by *election administrators shall* require two-factor authentication to access, apart from training modules.

4.1.13 All administrator passwords and decryption keys *shall* be given only to the designated authority representing the *election administrator* using a secure channel, independent from the technology or program (e.g., using hardware token for 2-factor authentication, inside a smartcard, or other option), who *shall* be responsible for the safe and secure keeping of the password and decryption keys.

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

4.1.14 The *online voting provider shall* allow authenticated administrators in the *municipality* to have password reset privileges.

4.1.15 Server-side components performing cryptographic operations, including key generation, *shall* use a cryptographic module that has undergone independent examination testing.

4.1.16 In the case where *voters*' votes are encrypted at the application layer on the client side, threshold encryption *shall* be used to generate the *election* decryption keys.

a. Each administrative *keyholder shall* receive relevant training.

b. Each administrative *keyholder shall* independently and locally generate its key share.

c. An independent third party who is knowledgeable in cryptographic secret sharing *shall* review the secret sharing procedure.

d. If passwords are used to secure the *election* decryption key shares, they *should* follow best practices as outlined in ITSAP.30.032.

4.1.17 *Online voting provider*s *shall* provide a cyber-incident response plan outlining how various cyber incidents will be handled, who will be notified of the incident, and under what circumstance. When possible, this plan *should* be integrated and aligned with the municipal cyber incident response plan, if one is available. Guidance for incident response plans is available in NIST 800-61.

4.1.18 The *online voting provider shall* make available documentation and/or training to system users with respect to threat detection, response, and need for failsafe plans.

a. The *online voting provider should* provide a sample failsafe plan which details how a democratic *election* will be conducted and decided in the event of detected online voting compromise or system failure. The plan *should* include acceptable levels of system downtime, *a service level agreement (SLA)*, and a mitigation plan to detect and recover from any issues.

b. *Election administrators shall* conduct "rehearsals" of system testing/*verification* shortly before the actual *election*, using local resources and volunteers. If issues or compromises are detected, the failsafe plan *shall* be referred to and/or refined.

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

4.2 Voter Security

4.2.1 The *online voting provider shall* advise how to protect from the possibility of recording a *voter* transaction if the *voter* is using a public *device* to access the *ballot* (e.g., a PC at a public library) based on industry best practices. The actual contents of the *voter*'s *ballot* (on any computer or *device*) *shall* be kept only in volatile memory, so that it will be automatically erased in the event of a power failure or re-booting.

4.2.2 Vote information *shall* not be written to long term storage on the *voter*'s *device*, even in encrypted form. Immediately after the *ballot* is sent to the vote server, or immediately after the *voter* clicks a "cancel" button, all records of the vote *shall* not be stored on the client-side *device*. This includes all cookies, temporary files, and beacons that could be associated with the *voter*'s selections or information that could be used to identify the *voter*.

4.3 Online voting provider security

4.3.1 The *online voting provider shall* conduct a third-party penetration test of the system that will be deployed in the *election*, at least once every 12 months.

4.3.2 The *online voting provider should* be responsible for all *independent 3rd party* contractor actions that they subcontract associated with online voting. The *online voting provider shall* exercise and perform due diligence when selecting third party *subcontractors*. All known risks associated with any third-party subcontractor *shall* be assessed, mitigated, documented, and provided to the *municipality* upon request. The *online voting provider should* be responsible for documenting and reporting on all adverse cyber-events, including with third parties.

4.3.3 *Online voting provider*s *shall* conduct testing with independent 3rd parties prior to the *election* wherein the testing simulates the traffic present on *election* day, if applicable. The results of such testing *shall* be provided to the *municipality*.

4.3.4 *Online voting provider*s *shall* have back-up *independent 3rd party* providers when applicable for all third-party services that they subcontract in the event of any incident where said service is not functioning or has limited functionality. If the *municipality* has 3rd party providers, the *municipality* is responsible for setting up back-up services.

5 Voter identity and vote authentication

5.1 Voter identity

5.1.1 In order to cast a vote via the online system, *voter*s *shall* prove to the *online voting service* that they are *eligible* to vote by using the authentication measure selected by the *election administrator*.

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

5.1.2 Before tallying the votes, the *online voting service should* ascertain that all votes cast and stored in the electronic ballot box have been cast by *eligible voter*s.

5.2 Vote authentication

5.2.1 The *online voting service shall* ensure that each *ballot* was counted and that only one vote per *voter* per office to be elected is included in the final tally, regardless of how the vote has been cast (e.g., online or on paper).

5.2.2 Authentication processes *shall* ensure that no attacker can cast a vote on behalf of another *voter* without having control over the *voter*s concerned:

a. Authentication information provided on a *Voter* Information Letter *should* be protected from unauthorized reading.

b. An attacker *should* not be able to cast a vote on behalf of another *voter* with the knowledge of fixed attributes of the *voter* (such as date of birth) and information contained within a *Voter* Information Letter.

6 Testing and auditability

6.1 Testing

6.1.1 The *online voting service shall* undergo *logic and accuracy testing*, overseen by the *election administrator*, prior to the *voting period*.

6.1.2 The parameters of the *logic and accuracy testing shall* be determined by the *election administrator* with the goal of establishing that the full range of possibilities of cast votes are counted correctly. This includes testing the accuracy of *ballot* classifications (e.g. valid or invalid *ballots*).

6.1.3 The parameters of the *logic and accuracy testing should* be made publicly available. *Logic and accuracy testing* procedures *should* be specified in a detailed public document.

6.1.4 A public demonstration of the voting website *should* be made available in advance of the *election* to allow *voter*s to gain familiarity with the interface. The configuration of the website *should* match the eventual live *election* website to the closest extent feasible.

6.1.5 The *online voting provider should* develop a policy for *coordinated vulnerability disclosure* (CVD).

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

6.1.6 *Election administrator*s may conduct or request additional threat, vulnerability, or penetration testing at their discretion. The *online voting provider*s will not have to bear the costs of such tests, and these *should* be properly planned not to jeopardize the calendar for delivering the *online voting service*. If an authorized representative is entrusted with the conduct of the tests, they may be asked to agree to confidentiality or responsible disclosure terms.

6.1.7 In addition to contracted penetration testing, terms and conditions for open-ended adversarial testing of the *online voting service should* be offered.

6.2 Auditability

6.2.1 The *online voting provider shall* offer to provide the *municipality* an audit procedure, testing manual, and training to enable the *municipality* to conduct audit tests.

6.2.2 The *online voting provider shall* ensure that all audit logs are secured and immutable to ensure that they cannot be modified after the fact.

6.2.3 The *online voting provider shall* provide a human-readable, non-rewritable audit log that records a *voter*'s actions (but not *ballot* selections) in the sequence that the steps were performed (such as logon, *ballot* cast, success of vote, logoff etc.).

6.2.4 The *online voting provider shall* maintain and prepare a chronological systems log of all processes that occur during the *voting period*. This log *should* be exportable for audit or retention purposes.

6.2.5 The *voter should* be able to verify that their intention is accurately represented in the vote and that the vote has not been altered after being cast. Any undue influence that has modified the vote *should* be detectable.

6.2.6 The *online voting provider should* provide evidence that each legitimate vote is accurately included in the *election results*, and that only *eligible voter*s' votes have been included in the results. The evidence *should* be verifiable by means that are independent from the online voting system. This evidence *should* be accessible to observers.

6.2.7 The counting of votes *should* be reproducible. The *online voting provider should* be able to provide sound evidence that the counting procedure has been performed satisfactorily, including through an independent audit.

6.3 Documentation

6.3.1 The *online voting provider should* provide, under the most favourable terms possible, access to the following information about the voting service, to the *election administrator*:

a. Technical documentation about the *online voting service*, including its architecture and technical specifications.

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

b. User handbooks for the operation of the *online voting service*.

c. Performance documentation including disclosure of denial of service, summary of past issues outages or vulnerabilities that have impacted the *online voting service* and how those have been addressed.

d. Assessment of the current threat environment and assessment of overall risk levels.

e. Source code, so that it may be inspected by the *election administrator* or, under certain circumstances, submitted to a third-party for review.

f. Attestation that all *voter information/data* and other records and artifacts from the *election* will be destroyed following the conclusion of the *election* or at the discretion of the *election administrator*.

g. Vulnerability assessments that have been completed in the 52 weeks before the *voting period*, that evaluates the security of the system, its vulnerabilities, and any fixes that have been implemented to mitigate the vulnerabilities.

6.3.2 Online voting providers shall provide documentation to the *municipality* on the processes qualified independent observers may use to *scrutineer* the *election* (e.g. review the evidence produced by the system, observe the *counting of votes*, recount procedures, etc.)

7 Access to online voting services and voter election information

7.1 Access, encryption, retention, and transfer of information

7.1.1 **Access and users**

7.1.1.1 Access and security permissions *should* use a role-based permissions framework that will enforce principles of least privilege and ensure that user*s* have access only to the resources and actions required for their role. The implementation of role-based permissions *should* match user access with job and task responsibility, and allow the *election administrator* to assign, modify and change user privileges for all *election official*s with maximum flexibility and granularity.

7.1.1.2 The *online voting service should* provide robust auditing capabilities to track user actions, including detecting unauthorized access attempts and attempts to escalate privileges or operate at a higher privilege level than assigned.

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

7.1.2 **Election results**

7.1.2.1 The *online voting service should* provide evidence to ascertain the correctness of the *election results*, for example, by providing independently verifiable cryptographic proof of a correct result. Where verifiable evidence is provided:

a. The evidence produced by the *online voting service shall* be verifiable by a qualified independent observer.

b. If the declared result is correct, the evidence provided *shall* be sufficient to convince independent observers of a correct result. If the declared result is incorrect, the evidence provided *shall* be sufficient to allow for independent observers to detect an incorrect result.

c. The evidence produced by the *online voting service shall* be accurate.

d. The *municipality shall* ensure that the process by which the results are verified is easily understood by non-technical users, *candidates*, and *election* officers to ensure trust in the results.

7.1.3 **Data retention**

7.1.3.1 All data captured by the *online voting provider*, or by an *independent 3rd party* hired by the *online voting provider*, *shall* be returned to the *municipality* or sanitized at the instruction of the *municipality* in accordance with the applicable legislation, unless keeping a copy of the data is in accordance with retention rules outlined in applicable legislation.

7.1.3.2 In certain circumstances during which the *online voting service* may be required to keep records longer than the prescribed period (such as a recount, or court proceeding, etc.), the *online voting provider shall* maintain all applicable records until determined by the *municipality*.

7.1.3.3 No proprietary, sensitive, or confidential information *shall* be transferred, shared, or published without written permission from the *municipality*.

7.1.3.4 Prior to collecting and processing data, *online voting providers shall*:

a. Conduct a Privacy Impact Assessment and Re-identification Risk Assessment of the proposed data usage activities. These assessments *shall* be conducted when there is a material change to the way in which data is collected, used or retained and in any event *shall* be conducted no less than once every three years.

b. Share the results of the Privacy Impact Assessment and Re-identification Risk Assessment, including any residual risks identified by these assessments, with *election administrator*s.

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

7.1.3.5 Where client authorization has been granted to process data, *election administrator*s *shall* provide notice of the collection and use of data and the purposes for which the data may be used.

NOTE: Municipalities retain full control and ownership of *election* data. *Online voting provider*s may, upon express written client authorization, collect, use and retain ("process") de-identified (including removal of IP addresses to anonymize the data) and aggregate information ("data"), which may include operating system and browser identifiers to ensure the safety and security of the internet voting platform and for product improvement purposes.

7.1.3.6 The *online voting service shall* implement technical measures to empower users to exercise control over the collection and/or use of data for product improvement purposes. At no time *shall* the authorization to process data include permission to engage in any activities which may re-identify or otherwise identify any person, or votes cast by any person.

7.1.3.7 *Online voting provider*s *shall* destroy data in accordance with applicable legislation, or a client's records retention schedule, if applicable, on the instructions of the client.

8 Secrecy of vote

8.1 Maintaining privacy, anonymity, integrity, and secrecy

8.1.1 The *online voting service shall* protect the integrity of the vote.

8.1.2 The *online voting service shall* protect the privacy of the *voter*'s information as used by the service. The vote *shall* be stored without any reference to the *voter*, and it *shall* not be possible to re-identify a *voter* and link them to their choice.

8.1.3 The *online voting service shall* ensure that the secrecy of the vote is always guaranteed, including during the casting, transfer, reception, collection, and tabulation of votes, as well as in the long-term.

8.1.4 The *online voting service shall* ensure that no one involved in the voting process can link or associate vote choices to an identifiable *voter* beyond what is discernible from the publicly reported *election results*. In cases where a *municipality* uses more than one voting method (online voting plus another method), those results *shall* be reported in a combined total.

8.1.5 The *online voting service shall* produce confirmation to the *voter* that their *ballot* was successfully cast, however, the *voter shall* not be able to prove with certainty to someone else how they voted.

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

9 Ballot design and accessibility

9.1 Useability and accessibility requirements

9.1.1 General

9.1.1.1 The *online voting service*'s interface *shall* be in standard scripting or rendering languages and *shall* not require the *voter* to perform installation of a plug-in or any additional hardware, software or firmware.

NOTE: Standard scripting refers to programming languages that are more frequently used.

9.1.1.2 The *online voting service shall* be designed with user-centred methods for a wide range of user/operators, including those with and without disabilities.

9.1.1.3 The *online voting service shall* comply with applicable accessibility legislation, and as a best practice *should* conform to the current Web Content Accessibility Guidelines (WCAG) required by the local jurisdiction.

9.1.1.4 The *online voting service shall* function on all *devices* and render effectively on any screen size without need for pinch and zoom and left/right scrolling. The *online voting service shall* also be responsive to input through both single and multi-touch screens, stylus, keyboard, and virtual keyboard. Where applicable, fields to be entered *should* allow for entry from drop down lists as well as direct keying.

9.1.1.5 The *online voting service shall* ensure the presentation of the order of contests and order of *candidates* is the same for all *voter*s, prior to selecting and casting their vote, in accordance with applicable legislation.

9.1.1.6 The *online voting service shall* ensure that the *voter*s' experience is consistent across all supported platforms and browsers. The *online voting service shall* provide an expected response to a sequence of actions by the *voter*, use identical terminology and abbreviations throughout, and any prompts, messages, or directives from the *online voting service should* always appear in the same place.

9.1.1.7 The technical design of the *online voting service shall* provide confirmation to a *voter* to indicate that their *ballot* has been cast successfully or unsuccessfully.

9.1.1.8 The *online voting service shall* inform any *voter*s who attempt to access the interface on an unsupported platform by displaying an explanatory error screen using plain language.

9.1.1.9 Where there is an applicable legislation to provide *voter*s the ability to decline, abstain, or spoil *ballots*, or for the *election administrator* to report on these items, then the system *should* allow for it.

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

9.1.1.10 Needs of *voter*s with disabilities or impairments *shall* be accommodated by the *online voting service* wherever possible, while facilitating independence. It *shall* be possible to create an audio version of the *ballot* to be read by the computer to a sight-impaired person, and the site *shall* be compatible with screen-reading technology.

9.1.1.11 The *online voting service shall* be designed to present an interface in any languages required by legislation in the jurisdiction, and/or as required by the *election administrator*.

9.1.1.12 The *online voting service shall* allow for the voting session to be halted at any point during the *voter*'s voting session, without saving any choices made to that point, nor striking the elector as having voted, until the *ballot* is cast. As a suggested best practice, the *online voting provider* and the *municipality should* develop a time out limit that balances useability with security.

9.1.1.13 Any audio-tactile interface of the *online voting service* designed for independent accessible voting *shall* be designed to provide the same capabilities to verify and cast a paper *ballot* as are provided by its normal visual interface.

9.1.1.14 The *online voting service shall* be designed to support rendering of *candidate* names using characters in Unicode blocks used in English, French and First Nations, Inuit and Métis languages, including: basic Latin, Latin-1 supplement and all Latin extensions; International Phonetic Alphabet extensions; combining diacritical marks; and unified Canadian Aboriginal syllabics and unified Canadian syllabics extended.

9.1.1.15 The *online voting provider shall* conduct usability and accessibility tests that address all user-facing features of the system.

NOTE: Accessibility tests check for all alternative access needs (e.g., for keyboard, voice and interoperability with assistive technologies such as magnifiers and screen readers).

9.1.2 **Accessibility and interoperability of reports and documentation**

9.1.2.1 The *online voting provider shall* provide all reports in accessible, interoperable, and commonly used formats, such as comma separated value (csv) files.

10 Bandwidth and network capacity

10.1 Technical network requirements and outages

10.1.1 The *online voting service shall* be available to *voter*s during the *voting period* and functioning properly during that time.

10.1.2 The *online voting provider shall* have a risk assessment and contingency plan in the event of network and power outages. The risk assessment *should* be conducted by an *independent 3rd party*. The contingency plan could be developed internally by the *online voting provider* or by an

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

independent 3rd party. Reports of the assessment and plan(s) *should* be made available to *election administrator*s upon request.

10.1.3 The *online voting provider shall* ensure that sufficient capacity is available to accommodate the entirety of the electorate during the *voting period*. The *online voting provider* and any independent 3rd parties hired by the *online voting provider shall* perform a load test simulating the highest rate of voting expected during the *voting period*, considering all overlapping *election*s that will occur on the *online voting service* during that time. The load test *shall* be performed on an agreed upon time prior to the start of the *voting period*, and the *online voting provider shall* provide a report to the *municipality* on the results of the load test.

11 Election Management/Administration

While the preceding sections of this standard provide technical requirements and specifications regarding online voting use, this portion outlines requirements for administering a municipal *election* with online voting services. The requirements in this final section of the standard, therefore, apply to the management of an *election* by administrators.

11.1 Staffing and personnel

11.1.1 The *online voting provider shall* ensure personnel are available to address any issues resulting from the *online voting service* throughout the duration of the engagement between the *municipality* and the *online voting provider*.

11.1.2 *Election administrator*s *should* ensure that any binding *independent 3rd party* subcontractors hired by the *online voting* provider are subject to the security and screening requirements of the jurisdiction.

11.1.3 *Election administrator*s *shall* protect against the possibility that a person may cast multiple *ballots* through different channels, where more than one voting channel is available to the *voter*. If *voter*s have choice in how they cast their *ballot*, it *shall* be ensured that only one vote per *voter* per office to be elected is included in the final tally, regardless of how the vote has been cast (e.g. online or on paper).

11.2 Risk assessment and security

11.2.1 The *municipality should* complete a Security Categorization (using the instructions in IT Security Risk Management: A Lifecycle Approach (ITSG-33) Annex 1) to determine potential risks, in advance of each *election*. It is a best practice for the Security Categorization to be approved and signed by the *Election Administrator* and/or best equivalent.

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

11.2.2 If the potential unmitigated risk in any area is predicted to be “High”, the *municipality should* consider not proceeding with online voting in the forthcoming *election*.

11.2.3 Municipalities *should* complete a Harmonized Threat Risk Assessment in advance of each *election*. Security controls *should* be considered for the following risks:

a. The assemblers used to convert assembly language to machine language were compromised.

b. The compilers and interpreters used to convert high-level language to assembly or machine language were compromised.

c. The source code in high level languages was compromised.

d. Binary software or firmware contains embedded compromises introduced via the use of unauthorized assemblers or compilers.

e. Hardware components contain embedded compromises introduced at the silicon die or micro-component level.

f. Cryptographic signing keys used to verify the integrity of software, firmware or hardware components have been compromised at source, negating the validity of signature checking.

g. Design, test, or operational documentation has been compromised, enabling undiscovered compromises to be delivered with the system.

h. An individual responsible for design, development, implementation, or maintenance of the system has been compromised, enabling undiscovered compromises to be delivered with the system.

i. Multiple individuals with system or electoral privileges have been compromised, enabling collusion on compromising the system or the results.

j. An out-of-band or sideband compromise has been implemented with the capability to transmit or receive secure data using non-typical electromagnetic, thermal, acoustic or optical paths.

11.2.4 Upon completion and ensuring it is safe to proceed, the report (also referred to as the residual risk rating) *should* be signed by the *Election Administrator* and/or best equivalent.

11.2.5 Any physical *devices* used to support all online voting activities *shall* be held in a physically secure location when not in use.

11.2.6 The *election administrator shall* plan and implement physical security measures prior to and following the *voting period* to prevent or provide evidence of any physical tampering with *devices* obtained by the *election administrator* to exclusively support online voting activities.

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

Bibliography

[1] Accessibility for Ontarians with Disabilities Act (2005).

[2] Budd, B., Gabel, C., & Goodman, N. (2019). Online voting in a First Nation in Canada: implications for participation and governance. In *Electronic Voting: 4th International Joint Conference, E-Vote-ID 2019, Bregenz, Austria, October 1–4, 2019, Proceedings 4* (pp. 50-66). Springer International Publishing.

[3] Cardillo, A., Akinyokun, N., & Essex, A. (2019). Online voting in Ontario municipal elections: a conflict of legal principles and technology? In *Electronic Voting: 4th International Joint Conference, E-Vote-ID 2019, Bregenz, Austria, October 1–4, 2019, Proceedings 4* (pp. 67-82). Springer International Publishing.

[4] 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.

[5] Elections Ontario, Office of the Chief Electoral Officer. (2012). Alternative Voting Technologies Report.

[6] Essex, A., & Goodman, N. (2020). Protecting Electoral Integrity in the Digital Age: Developing E-Voting Regulations in Canada. Election Law Journal, 19(2), 1-18.

[7] Essex, A., & Goodman, N. (2022). A Cyber-threat Analysis of Online Voting in Canada. In Holly Garnett and Michael Pal Eds., *Cyberthreats to Canadian Democracy*, McGill Queens University Press.

[8] Federal Chancellery of Switzerland. (2013). Federal Chancellery Ordinance on Electronic Voting.

[9] Goodman, N., Hayes, H. A., McGregor, R. M., Pruysers, S., & Spicer, Z. (2024). *Voting Online: Technology and Democracy in Municipal Elections*. McGill-Queen's Press-MQUP.

[10] Goodman, N., & Spicer, Z. (2019). Administering elections in a digital age: Online voting in Ontario municipalities. *Canadian Public Administration*, *62*(3), 369-392.

[11] Goodman, N. (2017). Online Voting: A Path Forward for Federal Elections. Privy Council Office, Government of Canada.

[12] Goodman, N & H. Pyman. (2016). ``Understanding the Effects of Internet Voting on Elections: Results from the 2014 Ontario Municipal Elections.'' Toronto: Centre for e-Democracy.

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

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

[15] State Electoral Office of Estonia. (2017). State Electoral Office of Estonia General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia.

[16] U.S. Election Assistance Commission. (2015). Voluntary Voting System Guidelines Version 1.1.

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

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

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.