ELECTIONSNWT ÉLECTIONSTNO

Electronic Voting Procedures

SECURITY OF SYSTEMS AND DATA

1. Service Provider

FR-1a The voting service shall make all reasonable efforts to detect and prevent each of the commonly cited classes of risk listed here:

i. Hacking – one or more outside hackers attempt to penetrate the election web servers or supporting infrastructure.

ii. Insider tampering – one or more insiders with varying levels of privileges attempt to observe or change the votes; this includes not only the service provider and Elections NWT, but also subcontractors including cloud providers, co-location providers, etc.

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

iv. Denial of Service (DoS) or Distributed Denial of Service (DDoS) – an attack on the voting service that renders the electronic voting platform inaccessible or unavailable for some or all voters.

v. Phishing – a deceptive technique where the attacker sends a fraudulent message designed to trick a person into revealing confidential, personal, or sensitive information to the attacker in order to deploy malicious software on the victim's infrastructure, such as ransomware.

vi. Client-side device security – including the inability of a compromised app or operating system to affect the functionality of the voting service.

vii. Insufficient IT resources – all contractors and subcontractors must ensure sufficient IT staff and resources, including proof of sufficient bandwidth capacity for:

1. Testing;
2. Regular monitoring and detection;
3. Proper capacity for timely cyber incident response; and
4. Project management.

viii. Weak authentication procedures – possibility for voter impersonation.

ix. Protections from voter data penetration, exfiltration and eavesdropping including:

1. Server-side eavesdropping by system administrators;
2. Server-side exfiltration of voter data by malware;
3. Server penetration and modification of voter data modification by external hackers;
4. Server-side voter data modification by privileged administrators;

5. Server penetration and exfiltration of voter data by external hackers.

x. Server-side logic/accuracy errors.

xi. Improper server-side network security configuration.

xii. Protection from voter data collection, anonymous or otherwise, by permanently deleting any data collected by their devices or system (see FR-2c below).

FR-1b The voting service shall provide 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.

FR-1c The voting service shall not store any data on servers located outside of Canada.

FR-1d All data shall be encrypted both in transit and at rest.

FR-1e The voting service shall include redundant firewalls, intrusion detection systems, verbose access logging, threat detection and prevention.

FR-1f The voting service shall adopt business continuity and data recovery plans that ensure the lowest Recovery Time Objective (RTO) and Recovery Point Objective (RPO) that are agreed on as adequate for the required voting service.

FR-1g The voting service shall have the ability to identify and indicate the severity of any suspicious voting activity or security breaches.

FR-1h The voting service's staff, including subcontractors, shall work on secured devices and networks which are encrypted and strong password-protected throughout the term of the contract with Elections NWT.

FR-1i An administrator password and/or encryption key shall be given to the individual(s) designated by the Chief Electoral Officer to be responsible for the safe and secure keeping of their password and encryption key.

FR-1j Server-side components performing cryptographic operations, including key generation, shall use a cryptographic module certified by the Cryptographic Module Validation Program (CMVP).

FR-1k The voting service shall freshly generate cryptographic keys for each election, and keys shall not be reused with other clients.

FR-1l The voting service must have a business continuity plan for the event of an internet failure, including built-in redundancy and geolocation.

FR-1m The voting service shall be designed with distributed, heterogenous architecture to avoid single-points-of-compromise.

2. Client-side Security

FR-2a Any administrative modules provided by the voting service for use by election administrators shall require multi-factor authentication to access.

FR-2b The voting service shall prevent from recording to memory a voter transaction if the voter is using a public machine, so that it will be automatically erased in the event of a power failure or re-booting.

FR-2c Votes shall not be written to long-term storage on the client machine, 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 be deliberately erased from the voter's computer. This would include all cookies, temporary files and beacons used in the voting process.

3. Third Party Contractor Security

FR-3a The voting service shall be responsible for all ways in which third-party contractor actions might affect the operation of the system associated with the electronic ballot. The voting service shall be responsible for ensuring all risks associated with the third-party are documented, assessed, mitigated and available to Elections NWT upon request.

FR-3b The voting service shall conduct testing with third-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 Elections NWT.

FR-3c Any third-party contractor hired by the voting service shall have proof of integration with the voting service.

FR-3d Any third-party contractor hired by the voting service shall detect and prevent each type of commonly cited classes of risk listed below:

i. Collection of voter data – the voting service shall not collect voter data. If any such data is collected it is to be returned to Elections NWT or destroyed following the vote.

ii. All elements included for the voting service listed above.

FR-3e Any third-party contractor hired by the voting service shall provide proof of testing of its security, its vulnerabilities, and any fixes that have been implemented to mitigate the vulnerabilities.

FR-3f The voting service shall have back-up third-party providers for all third-party services in the event of a technical issue where said service is either not functioning or is limited in its function.

VOTER IDENTITY AND VOTE AUTHENTICATION

4. Voter Identity

FR-4a In order to be eligible to cast a vote electronically, voters shall apply for an absentee ballot through the DataFix portal hosted on the Elections NWT website.

FR-4b The voting service must be able to seamlessly integrate with DataFix's VoterView, a secure web-based Voters' List management application.

5. Vote Authentication

FR-5a The voting service shall ensure that each electronic ballot was counted and that a voter can only cast a single ballot.

FR-5b The voting service must prevent credentials from successfully being used more than once.

FR-5c The voting service must prevent the addition of fake votes from both external users and system administrators.

FR-5d The voting service must implement adequate measures for detecting any attempt to delete a vote from the ballot box.

FR-5e The voting service must provide the method for ensuring that the authenticity and integrity of the ballot box can be verified before accepting it for the count.

FR-5f The voting service must generate reports that ensure the total number of voters using the internet vote channel is equal to the total number of electronic votes cast, grouped by electoral district.

VERIFICATION, TESTING, AND AUDITABILITY

6. Voter verification

FR-6a After the election is complete, the voting service should allow voters, by means of a unique voting receipt, to verify if their vote was accurately recorded and to confirm that their vote was not altered or tampered with and that it was properly counted.

FR-6b Voters should be able to verify the authenticity of the voting receipt generated to enable the verification of the results.

FR-6c A voting receipt must preserve the vote's secrecy so that the voter's choice of candidate cannot be deduced, and the voter can not prove who they had voted for to a third-party.

FR-6d The verifiability service must be available for one week following the close of polls on Polling Day (8pm Mountain time).

7. Testing

FR-7a The voting service shall undergo logic and accuracy testing, overseen by a representative of Elections NWT, prior to the election period. The parameters of the logic testing are as set by Elections NWT.

FR-7b Elections NWT can conduct or request additional threat or penetration testing at their discretion.

FR-7c The voting service shall provide proof to Elections NWT that the voting service has been subject to a third-party penetration test that evaluates the security of the system, its vulnerabilities, and proof that fixes that have been implemented to mitigate the vulnerabilities, as well as any proof of other work to improve the security of the system.

8. Auditability

FR-8a The voting service shall provide Elections NWT an audit procedure, testing manual and training to enable Elections NWT to conduct audit tests.

FR-8b The voting service must include an audit log that records a voter's actions, but not ballot selections, in the sequence that the steps were performed.

FR-8c The voting service shall maintain and prepare a printable chronological systems log of all processes that were performed by system administrators during the voting period.

FR-8d The voting service shall provide access logs to the election administrator.

FR-8e Storage of audit logs on electronic media shall be protected using cryptographic authentication to prevent tampering.

FR-8f The voting service shall provide a solution that will allow for a physical accounting of the votes cast electronically during a judicial recount, that shall allow for an accounting of individual votes cast, without identifying the voter.

ACCESS, RETENTION AND TRANSFER OR INFORMATION

9. Administrator Access

FR-9a The voting service shall provide multiple access levels so that Elections NWT administrators and voting service provider staff have access to only those aspects of the voting service that their duties require.

FR-9b The voting service shall be designed to allow the election administrator to enable or disable functions as required.

10. Data retention

FR-10a All data captured by the voting service, or in the possession of the voting service, shall be returned to Elections NWT or destroyed following the conclusion of the election. Furthermore, such information or data remains the property of Elections NWT and shall not be used by the voting service for financial or personal gain. Any data shared with the voting service in order to deliver the electronic ballot shall be subject to the same requirements as applicable.

FR-10b The voting service may be required, upon request of the Chief Electoral Officer of the Northwest Territories, to keep records longer than the prescribed period in the event that a recount requires those records to be maintained for a longer period of time.

FR-10c No proprietary, sensitive or confidential information shall be transferred, shared or published without written permission from the Chief Electoral Officer of the Northwest Territories.

11. Maintaining privacy, anonymity, integrity and secrecy

FR-11a The voting service shall protect the privacy, anonymity, integrity and secrecy of each voter's ballot by severing the vote from the voter.

FR-11b The voting service must not display the vote selection after the successful completion of casting the vote.

FR-11c The voting service must protect the secrecy of the cast vote, along with the voter's identity, by digital signatures, encryption and cryptographic means.

FR-11d The voting service must be capable of protecting the cast votes, in transit and in the ballot box, from manipulation by external and internal attackers.

FR-11e The voting service must guarantee that there is no possibility for connection between the voter and the vote cast and that it is impossible to correlate the order in which the votes were decrypted with the order in which they were cast.

FR-11f The voting service must guarantee that a cast ballot is secret in front of any third-party, including system administrators and potential hackers that break through the conventional security measures protecting the voting platform.

FR-11g The voting service must not allow the voter to retain a copy of their vote. It should not offer the functionality of printing, saving or storing the vote or part of the screen on which the vote is visible.

FR-11h The voting service must guarantee that the monitoring tools cannot compromise the voter's privacy and election accuracy. The voting service must prevent anybody, even privileged managers or auditors, to correlate votes with voters.

BALLOT DESIGN AND ACCESSIBILITY

13. Ballot Design and Accessibility

FR-12a The voting service's interface shall be in standard scripting or rendering languages and shall not require the installation of an end-client or plug-in of any additional hardware, software or firmware.

FR-12b Presentation of the candidate's names must support the use of multiple language characters (e.g., accents and special characters).

FR-12c The ballot will include photos of the candidates, where they have been provided.

FR-12d The voting service shall be intuitive and easy-to-use for all demographics, including, but not limited to, persons with disabilities. To achieve this end, the voting service should conform to the Web Content Accessibility Guidelines (WCAG).

FR-12e The 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 voting service must also be responsive to input through both single and multi-touch screens, stylus, keyboard, and virtual keyboard.

FR-12f The voting service shall ensure the presentation of the order of candidates is the same for all voters, prior to making a selection and casting their vote.

FR-12g The voting service must clearly distinguish to the voter the selected candidate from the un-selected ones.

FR-12h The voting service shall ensure that the voters' experience is consistent across all supported platforms and browsers. The voting service shall provide an expected response to a sequence of actions by the voter, use identical terminology and abbreviation throughout, and any prompts, messages or directives from the voting service should always appear in the same place.

FR-12i The voting service shall adhere to responsive web design principles.

FR-12j The voting service must confirm to the voter that their vote is deposited in the ballot box and that the voting process has been completed successfully.

FR-12k The voting service shall provide the option to decline a ballot, and include the total number of declined ballots by electoral district in the results.

FR-12l Needs of voters with disabilities or impairments shall be accommodated by the voting service wherever possible, while facilitating independence. The site shall be compatible with screen-reading technology.

FR-12m The voting service shall be designed to present an interface in any language required by Elections NWT.

FR-12n The 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.

FR-12o The voting service shall be designed to not permit any on screen marketing, electioneering or campaigning.

FR-12p The voting service shall be designed to provide accessible guidance in multiple formats to voters who attempt to access the platform using an unsupported device.

FR-12q The voting service shall be designed to provide a visual or auditory confirmation that the vote was received and cast successfully.

FR-12r The voting service shall be designed to provide a visual or auditory notification to the voter that the vote was not received, and steps to retry or troubleshoot the issue.

BANDWIDTH AND NETWORK CAPACITY

13. Technical network requirements and outages

FR-13a The voting service shall be available to voters during the voting period and function properly during that time.

FR-13b The voting service shall perform a risk assessment and develop a contingency plan in the event of network or power outages.

FR-13c The voting service shall have back-up servers to ensure continuity of service.

FR-13d The voting service shall ensure that additional bandwidth capacity is available to handle the influx of electronic voters during the voting period, especially during higher traffic periods, such as on election day.

FR-13e The voting service shall perform load balancing and stress tests simulating extreme demand conditions, prior to the first day of advance voting.

FR-13f Backup service providers must be contracted well in advance as part of the business continuity plan.

14. REPORTING

FR-14a The voting service must be able to generate, by Electoral District, the total count and a list of the elector IDs and names of all voters who have registered to vote electronically and their voting status (voted or not voted by internet), as of date. Report information must be downloadable in CSV format at least, and upon Elections NWT request.

FR-14b The voting service must be able to generate, upon Election NWT's request, a list of the names of all voters who have voted using the electronic voting channel, showing their electoral district, elector ID and the date and time of the voting action, within the specified requested dates and time (from-to) period. Report information must be downloadable in CSV format at least.

FR-14c The voting service should be able to generate custom reports as requested by Elections NWT to validate the accuracy and correct application of the exchanged information.

15. COUNTING

FR-15a The voting service must securely store off-line all the votes cast until the close of polls on election day and the start of the count.

FR-15b The voting service shall be designed to ensure all voter information/data and ballot counting results are protected and backed-up according to security protocols.

FR-15c The tallying process must ensure that it is impossible to correlate the order of the votes with the order they were cast or to connect the cast vote to the identity of the voter casting it.

FR-15d The tallying process must guarantee that it is impossible to correlate any voter verification information (voting receipts) with the voting options selected within the ballot.

FR-15e For each Electoral District where an election is running, the voting service must count the electronic votes cast for each candidate running in the district, and any declined ballots.

FR-15f For each Electoral District, the voting service must generate a "Statement of Vote" report showing the electronic vote count per candidate, the count of declined votes, the total number of voters who voted electronically, and the total number of electronic votes cast for each Electoral District.

FR-15g The voting service must be able to re-generate the vote count upon request (for recount purposes).

FR-15h The voting service shall be designed to prevent any information regarding the results to be generated prior to the end of the voting period.

FR-15i The voting service shall be designed to prevent the counting of unverified votes or any unauthorized user accounts.

FR-15j The voting service shall be designed to generate reports at the discretion of the election administrator, on an as needed basis (e.g., the number of voters, or the strike-off list).

FR-15k The voting service shall be designed to detect and prevent the deletion of votes.

15. DOCUMENTATION

FR-16a The voting service shall provide the following documentation, in an accessible format, to the election administrator:

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

ii. An assessment of the current threat environment and an assessment of overall risk levels.

iii. 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 Chief Electoral Officer.

iv. Vulnerability assessments that have been completed within one year of the election period.