Voluntary Voting System Guidelines 2.0

Principles and Guidelines

Principle 1: HIGH QUALITY DESIGN

The voting system is designed to accurately, completely, and robustly carry out election processes.

1.1 - The voting system is designed using commonly-accepted election process specifications.

1.2 - The voting system is designed to function correctly under all realistic operating conditions.

1.3 - Voting system design supports evaluation methods enabling testers to clearly and easily distinguish systems that correctly implement specified properties from those that do not.

Principle 2: HIGH QUALITY IMPLEMENTATION

The voting system is implemented using high quality best practices.

2.1 - The voting system is implemented using trustworthy materials and methods.

2.2 - The voting system is implemented using best practice user-centered design methods, for a wide range of representative voters and poll workers, including those with and without disabilities.

2.3 - Voting system logic is clear, meaningful, and well-structured.

2.4 - Voting system structure is modular, scalable, and robust.

2.5 – The voting system supports system processes and data with integrity.

2.6 - The voting system handles errors robustly and gracefully recovers from failure.

2.7 - The voting system performs reliably in intended environments.

Principle 3: TRANSPARENCY

The voting system and voting processes are designed to provide transparency.

3.1 - The documentation describing the voting system design, operation, accessibility features, security measures, and other aspects of the voting system can be easily read and understood by election officials, testing labs, and independent auditors.

3.2 - The processes and transactions, both physical and digital, associated with the voting system are readily available for inspection.

3.3 - The operations of the voting system are easy for the public to understand and verify during pre-election setup and post-election audits.

Principle 4: INTEROPERABILITY

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

4.1 - Voting system data that is imported, exported, or otherwise reported, is in an interoperable format.

4.2 - Standard, publicly-available formats for other types of data are used, where available.

4.3 - Widely-used hardware interfaces and communications protocols are used.

4.4 - Commercial-off-the-shelf (COTS) devices can be used when their usage meets applicable requirements.

Principle 5: EQUIVALENT AND CONSISTENT VOTER ACCESS

All voters can access and use the voting system regardless of their abilities, without discrimination.

5.1 - Voters have a consistent experience throughout the voting process in all modes of voting.

5.2 - Voters receive equivalent information and options in all modes of voting.

Principle 6: VOTER PRIVACY

Voters can mark their ballot and verify, and cast their vote selections privately and independently.

6.1 - The voting process preserves the privacy of the voter's interaction with the ballot, modes of voting, and vote selections.

6.2 - Voters can mark their ballot and verify and cast their vote selections or other associated cast vote record, without assistance from others.

Principle 7: MARKED, VERIFIED, AND CAST AS INTENDED

Ballots and vote selections are presented in a clear, understandable way and can be marked, verified, and cast by all voters.

7.1 - **PERCEIVABLE** - The default voting system settings for displaying the ballot work for the widest range of voters, and voters can adjust settings and preferences to meet their needs.

7.2 - **OPERABLE** - Voters and poll workers can use all controls accurately, and voters have direct control of all ballot changes.

7.3 - **UNDERSTANDABLE** - Voters can understand all information as it is presented, including instructions, messages from the system, and error messages.

Principle 8: ROBUST, SAFE, USABLE, AND ACCESSIBLE

The voting system and voting processes provide a robust, safe, usable, and accessible experience for all users.

8.1 - The voting system's hardware and accessories protect voters from harmful conditions.

8.2 - The voting system meets currently accepted federal standards for accessibility.

8.3 - The voting system is measured with a wide range of representative voters and poll workers, including those with and without disabilities, for effectiveness, efficiency, and satisfaction.

Principle 9: AUDITABILITY

The voting system is auditable and enables evidence-based elections.

9.1 - An undetected error or fault in the voting system software or hardware cannot cause an undetectable change in election results.

9.2 - The voting system produces records that provide the ability to check whether the election outcome is correct and, to the extent possible, identify the root cause of any irregularities.

9.3 - Voting system records are resilient in the presence of intentional forms of tampering and accidental errors.

9.4 - The voting system supports efficient audits.

Principle 10: BALLOT SECRECY

The voting system protects the secrecy of voters' ballot selections.

10.1 - Ballot secrecy is maintained throughout the voting process.

10.2 - The voting system does not produce records, notifications, information about the voter or other election artifacts that can be used to associate the voter's identity with the voter's intent, choices, or selections.

Principle 11: ACCESS CONTROL

The voting system authenticates administrators, users, devices, and services before granting access to sensitive functions.

11.1 - Access privileges, accounts, activities, and authorizations are logged, monitored, and reviewed periodically and modified as needed.

11.2 - The voting system limits the access of users, roles, and processes to the specific functions and data to which each entity holds authorized access.

11.3 - The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations.

11.4 - Default access control policies enforce the principles of least privilege and separation of duties.

11.5 - Logical access to voting system assets are revoked when no longer required.

Principle 12: PHYSICAL SECURITY

The voting system prevents or detects attempts to tamper with voting system hardware.

12.1 - Any unauthorized physical access to the voting system other hardware leaves physical evidence.

12.2 - The voting system only exposes physical ports and access points that are essential to voting operations, testing, or auditing.

Principle 13: DATA PROTECTION

The voting system protects sensitive data from unauthorized access, modification, or deletion.

13.1 –The voting system prevents unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records.

13.2 - The source and integrity of electronic tabulation reports are verifiable.

13.3 - All cryptographic algorithms are public, well-vetted, and standardized.

13.4 - The voting system protects the integrity, authenticity, and confidentiality of sensitive data transmitted over all networks.

Principle 14: SYSTEM INTEGRITY

The voting system performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

14.1 - The voting system uses multiple layers of controls to provide redundancy against security failures or vulnerabilities.

14.2 - The voting system limits its attack surface by reducing unnecessary code, data paths, physical ports and by using other technical controls.

14.3 - The voting system maintains and verifies the integrity of software, firmware, and other critical components.

14.4 - Software updates are authorized by an administrator prior to installation.

Principle 15: DETECTION AND MONITORING

The voting system provides mechanisms to detect and remediate anomalous or malicious behavior.

15.1 - Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing.

15.2 - The voting system generates, stores, and reports to the user or election official, all error messages as they occur.

15.3 - The voting system employs mechanisms to protect against malware.

15.4 - A voting system with networking capabilities employs appropriate, well-vetted modern defenses against network-based attacks, commensurate with current best practice.