DRAFT VVSG 2.0 Principles and Guidelines

03/27/2017

Table of Contents

General Principles and Guidelines

Principle 1: CORRECT IMPLEMENTATION

Completely and accurately carry out election processes.

1.1 - Carry out election operations completely and accurately across the entire election process – supporting the integrity and maintainability of the entire process and data across hardware, software, telecom, data, and/or other technology layers of the system.

1.2 - Carry out election processes completely and accurately under realistic operating conditions – including correct operation under expected workloads, expected environmental conditions, and means of data transfer.

1.3 - Carry out election processes completely and accurately carry across the entire system lifecycle – ensuring election processes remain correct in definition and execution no matter whether how the system lifecycle processes may change (i.e., specification, implementation, testing, operations, or maintenance processes) and regardless of whether this is occurring in hardware, software, telecom, data, and/or other technology layers of the system.

Principle 2: HIGH-QUALITY CONSTRUCTION

Construct to maximize quality.

2.1 - Use trustworthy materials, methods, standards, and best practices – including accepted and appropriate tools/standards for constructing hardware and software, protocols for constructing and performing telecommunications, as well as best practices for quality assurance and configuration management.

2.2 - Organize the elements and logic of the system meaningfully – ensuring logic that is clear, meaningful, and well-structured; system organization that is simple, modular, and robust to change; and hardware, telecom, data, and

related infrastructure that can support system processes and functions with integrity.

2.3 - Handle errors actively and appropriately, recovering from failure gracefully – processing or avoiding well-known errors and/or software bugs; and avoiding single points of failure that could cause complete loss of voting capabilities.

2.4 - Perform accurately and reliably in intended environments – ensuring system is free of well-known security vulnerabilities; is able to protect against threats to its software, execution, and/or environment; and can maintain accuracy, data integrity, durability, and safety across all logical and/or physical components and materials.

2.5 - Support auxiliary functions necessary for operations and transparency such as for supporting auditing and testing – ensuring these aims are achievable via supporting structures, functions, and data; are implemented in software, hardware, telecom, and/or other infrastructure; and can support accurate identification, tracking, and management of hardware, software, and data across the system lifecycle.

Principle 3: EASE OF EVALUATION

Support clear evaluation by reviewers.

3.1 - Ensure reviewers can clearly identify all essential elements of a specified system in evaluated systems – including identification of unique election/auxiliary processes and functions; wherever they are implemented in software, hardware, telecom, data, and/or other technology layers of the system; and with an ability to record and track these identifications.

3.2 - Ensure reviewers can clearly distinguish correct from incorrect system configurations in evaluated systems wherever they are implemented in software, hardware, telecom, data, and/or other technology layers of the system; and with an ability to record and track these distinctions.

Interoperability Principles and Guidelines

Principle 1: TRANSPARENT

The voting system provides for transparency.

1.1 - The processes and transactions associated with the voting system are easy for the public to understand and verify.

1.2 - Voting system data is easily accessed via imports/exports and reports.

1.3 - Data reported by the voting system is in a publicly documented format.

1.4 - Data used in critical device operations such as for cast vote records, tabulations, and event logs includes all elements necessary for verification of the data, and analysis and auditability of the operations.

Principle 2: SCALABLE

The voting system is scalable.

2.1 - The system provides sufficient technical and physical capacity to accommodate large and complex ballot styles, growing language needs, and large numbers of voters and precincts and consolidation of elections with local districts and municipalities.

2.2 - The system provides the ability to adapt to different election types, environments, and changing regulatory requirements.

Principle 3: INTEROPERABLE COMPONENTS

Components of the voting system are interoperable.

3.1 - Voting system data is in an interoperable format that is common across manufacturers and documented for each device by the manufacturer.

3.2 - Formats for other types of data use industry standard formats where applicable, but in any case, use formats that are publicly available.

3.3 - Components of voting systems interoperate without the need to replace the entire system or undertake costly system modifications or impact security.

3.4 - Widely used hardware interfaces and communications protocols are used where possible.

Human Factors Principles and Guidelines

Principle 1: EQUIVALENT AND CONSISTENT

All voters have access to mark and cast their ballot as intended, regardless of their abilities, without discrimination.

1.1 - Provide voters with a consistent experience of the voting process in all modes of voting.

1.2 - Provide voters with equivalent information and options in all modes of voting.

Principle 2: CAST AS MARKED

Ballots are cast as marked, both secretly and privately.

2.1 - The voting process preserves the secrecy of the ballot.

2.2 - The voting system ensures that ballot selections, interface options, voter identity and information about voters are kept private.

2.3 - The voting system supports the voter in marking the ballot accurately.

2.4 - The voting process helps voters avoid errors that invalidate their ballot, including blank ballots, undervotes, overvotes, and marginal marks.

Principle 3: MARKED AS INTENDED

Ballots are presented in a clear, understandable way, and are operable by all voters.

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

3.2 OPERABLE - Voters and poll workers are able to use all controls accurately, and all ballot changes are made with the direct control of the voter.

3.3 UNDERSTANDABLE - Voters can understand all information as it is presented.

3.4 ROBUST - The voting systems hardware and accessories support usability and accessibility requirements while protecting voters from harmful conditions.

Principle 4: TESTED FOR USABILITY

Meets performance standards for usability and accessibility.

4.1 - Completed systems are tested using a wide range of representative voters and poll workers, including those with and without disabilities to measure effectiveness, efficiency, and satisfaction (called "summative usability testing").

Principle 5: MEETS WEB ACCESSIBILITY STANDARDS

Browser-based systems meet web accessibility standards in addition to voting standards.

5.1 - When a voting system uses standard web software platforms (HTML or native apps), the voting system meets all requirements in WCAG 2.0 Level AA any applicable requirements in the VVSG.

Security Principles and Guidelines

Principle 1: AUDITABILITY

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

1.1 - An undetected error or fault in the voting systems software is not capable of causing an undetectable change in election results.

1.2 - 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.

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

1.4 - The voting system supports efficient audits.

Principle 2: BALLOT SECRECY

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

2.1 - Ballot secrecy is maintained throughout the voting process.

2.2 - Records produced by the voting system do not reveal how a voter voted.

Principle 3: ACCESS CONTROL

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

3.1 - The voting system identifies users, roles and/or processes to which access is granted and the specific functions and data to which each entity holds authorized access.

3.2 - The voting system supports authentication mechanisms and allows administrators to configure them.

3.3 - Default access control policies enforce the principle of least privilege.

Principle 4: PHYSICAL SECURITY

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

4.1 - Any unauthorized physical access to the voting system, ballot box, ballots, or other hardware, leaves physical evidence.

4.2 - Voting systems only expose physical ports and access points that are essential to voting operations, testing, or auditing.

Principle 5: DATA PROTECTION

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

5.1 - Voting systems prevent unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records.

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

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

5.4 - Voting systems protect the integrity, authenticity and confidentiality of sensitive data transmitted over all networks.

Principle 6: SOFTWARE INTEGRITY

Voting systems prevent the unauthorized installation or modification of firmware, software, and critical configuration files.

6.1 - Only software that is digitally signed by the appropriate authorities is installed on the voting system.

6.2 - The authenticity and integrity of software updates are verified by the voting system prior to installation and authorized by an administrator.

Principle 7: DETECTION AND MONITORING

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

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

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

7.3 - Voting systems employ mechanisms to protect against malware.

7.4 - If the voting system contains networking capabilities, it employs appropriate modern defenses against network-based attacks.