Auditability – The voting system is auditable.

- An undetected error or fault in the voting system's software is not capable of causing an undetectable change in election results.
- 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.
- Voting system records are resilient in the presence of intentional forms of tampering and accidental errors.
- The voting system supports efficient audits.

Relevant Notes on changes to the *Auditability* Principle & Guidelines:

- Removed the portion about a "robust evidence trail to verify the election outcome" from the principle description.
- Reworked the final guideline based to explicitly, and plainly, state that the voting system supports efficient audits. Ron Rivest has early thoughts on what supporting "efficient audits" means.
- Added language to ensure where possible, the election records can help identify the source of errors or faults.

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

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

Relevant Notes on changes to the *Ballot Secrecy* Principle & Guidelines:

- The second guideline was updated based on discussion from the mailing list. The phrase "transmitted over the network" was removed.

Ballot Integrity - The voting system protects cast vote records from modification or deletion.

- Cast vote records are stored in a manner that does not reveal how a particular voter voted.
- Voting systems preserve the integrity of voter selections when transmitted over networks.

Relevant Notes on changes to the *Ballot Integrity* Principle & Guidelines:

- **This principle is to be deleted and will no longer be reflected on the TWIKI website.**
- All the guidelines and concepts were found within other principles, such as the first guideline under the Data Protection principle.

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

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

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

Relevant Notes on changes to the *Access Control* Principle & Guidelines:

- None.

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

- Any unauthorized physical access to the voting system, ballot box, ballots, or other hardware, leaves physical evidence.
- Voting systems only expose physical ports and access points that are essential to voting operations, testing, or auditing.

Relevant Notes on changes to the *Physical Security* Principle & Guidelines:

- Incorporated leaving physical evidence to the ballot box and ballot per the suggestion of the Working Group

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

- Voting systems prevent unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records.
- The source and integrity of electronic tabulation reports are verifiable.
- All cryptographic algorithms are public, well-vetted, and standardized.
- Voting systems protect the integrity, authenticity and confidentiality of sensitive data transmitted over all networks.

Relevant Notes on changes to the *Data Protection* Principle & Guidelines:

- Combined the communications security guidelines into the data protection section, by inserting the Communications security Principle description.

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

- The integrity of network communications must be cryptographically verified.
- Telecommunications must be encrypted and authenticated to protect against eavesdropping and data manipulation.
- Wireless channels must be encrypted and authenticated to protect against eavesdropping and data manipulation.

Relevant Notes on changes to the *Communications Security* Principle & Guidelines:

- **This principle is to be deleted and will no longer be reflected on the TWIKI website.**
- The Principle description was inserted into the Data Protection section.

Software Quality - Voting system software is free of defects or vulnerabilities that may significantly disrupt the election, compromise election integrity, or violate ballot secrecy.

- Voting systems must be implemented using modern, high-level languages that provide common control constructs.
- Voting system software must adhere to published, credible coding conventions.
- Voting system software must be designed in a modular fashion.
- Voting system software source code must be documented.
- Voting system software must detect, avoid and prevent well-known types of errors.

Relevant Notes on changes to the *Software Quality* Principle & Guidelines:

- **This principle is to be deleted and will no longer be reflected on the TWIKI website.** This principle and associated guidelines may be better suited for a different group. Ben Long of NIST is currently working in this area.
- Many of the guidelines are related to current VVSG requirements, and are style based.
- Since manual software review can be expensive, and this group is focusing on evidence trails and audits, it may be best to err on the side of fewer guidelines.

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

- Voting systems provide methods to verify only authorized software is present on voting systems.
- The authenticity and integrity of software updates are verified by the voting system prior to installation and authorized by an administrator.

Relevant Notes on changes to the *Software Integrity* Principle & Guidelines:

- Added “unauthorized” to the principle description based on WG feedback.
- No specific mention of whitelisting, although this seems like what the guidelines are hinting at.
- Removed the last guideline. It was unclear what “identified” software and equipment meant.

Detection & Monitoring - The voting system provides mechanisms to detect and remediate anomalous or malicious behavior.

- Voting system equipment records important activities through event logging mechanisms.
- The voting system generates, stores, and reports to the user or election official, all error messages as they occur.
- Voting systems employ mechanisms to protect against malware.
- Voting systems monitor network traffic to identify and protect against attempted attacks.

Relevant Notes on changes to the *Detection & Monitoring* Principle & Guidelines:

- Does monitoring network traffic mean that a firewall is part of a voting system?

- There's been a suggestion that the guideline on malware be removed, since it might be covered under the software integrity principle. I am waiting to discuss this on the next WG call before proceeding.
- Removed "System and election logs are protected from unauthorized modification or deletion" since it was redundant.

The following are concepts discussed with the Working Group that are not reflected within the principles and guidelines:

- Vulnerability management
- Timeliness of software updates
- Ensuring only supported software, aka actively maintained software, is used on the voting system
- Transparency of voting system software – the concept that voting system software should be available for review to the public