Principle 10
Ballot Secrecy

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

Requirements for Principle 10

10.1 - Ballot secrecy is maintained throughout the voting process.

10.1-A – System use of voter information

10.2 - The voting system does not contain nor 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.

10.2.1 – Voter associations
10.2.1-A – Direct voter associations
10.2.1-B – Indirect voter associations
10.2.1-C – Use of indirect voter associations
10.2.1-D – Election worker selection of indirect associations
10.2.1-E – Isolated storage location
10.2.1-F – Confidentiality for indirect association
10.2.2 – Identification in vote records
10.2.2-A – Identifiers used for audits
10.2.2-B – No voter record order information
10.2.2-C – Identifying information in voter record file names
10.2.2-D – Non-memorable identifiers and associations
10.2.2-E – Aggregating and ordering
10.2.3 – Access to cast vote records (CVR)
10.2.3-A – Least privilege access to store
10.2.3-B – Limited access
10.2.3-C – Authorized access
10.2.3-D – Digital voter record access log
10.2.4 – Voter information in other devices and artifacts
10.2.4-A – Voting information in receipts
10.2.4-B – Ballot secrecy for receipts
10.2.4-C – Logging of ballot selections
10.2.4-D – Activation device records

10.1 - Ballot secrecy is maintained throughout the voting process.

10.1-A – System use of voter information

The voting system must be incapable of accepting, processing, storing, and reporting identifying information about a specific voter, with the exception of blank ballot distribution and online ballot marking systems.

Discussion

Examples include first name, last name, address, driver's license, and voter registration number. The voting system cannot prevent a voter from self-identifying within write-in fields.

Notes: 10.1-A would preclude many remote electronic ballot delivery systems from being included as a part of the voting system. These systems may authenticate voters with username and password, which often has first name, last name, and email within the same system.

10.2 - The voting system does not contain nor 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.

10.2.1 – Voter associations

10.2.1-A – Direct voter associations

The voting system must not create or store direct associations between a voter's identity and their ballot.

Discussion

A direct voter association would be the voting system storing that John Smith voted for George Washington. Other examples of a direct association would include tying ballot selections to a social security number, voter identification number, or driver's license number. (This is not an exhaustive list of direct voter association examples.)

10.2.1-B – Indirect voter associations

Only E2E voting systems may use indirect associations; other systems must not.

Discussion

Certain channels of voting require indirect associations so that ballots can be removed before the ballot is read and counted. Some reasons include signature mismatch or death of a voter. Once a ballot is read and counted, the ballot is permanently stripped of its identifier. The most common example of indirect association would be a randomly generated number. Ballots with indirect associations are not considered read or counted until the association is removed.

Applies to: E2E voting system architectures

10.2.1-C – Use of indirect voter associations

The voting system must only use indirect associations for situations when a voter needs to fill out a ballot before their eligibility is determined.

Discussion

Certain channels of voting require indirect associations so that ballots can be removed before casting for a variety of reasons including signature mismatch or death of a voter. The act of casting the ballot permanently strips it of an identifier.

The most common example of indirect association would be a randomly generated number. Ballots with indirect associations are not considered cast until the association is removed.

Best practice would ensure that indirect voter associations are only available to authorized election personnel.

Applies to: E2E voting system architectures

10.2.1-D – Election worker selection of indirect associations

When the use of an indirect association is needed, an election worker must select the option for using an indirect association at the beginning of each new voting session.

Applies to: E2E voting system architectures

10.2.1-E – Isolated storage location

Ballots that are not cast and contain an indirect association must be stored in separate storage locations from cast ballots.

Discussion
Ballots that contain an indirect association are not considered cast. Cast ballots and ballots having their eligibility considered need to be kept separate from each other. Although not the only way of meeting this requirement, one example would be storing cast ballots in a different directory from ballots not yet cast.

Applies to: E2E voting system architectures

10.2.1-F – Confidentiality for indirect association

Ballots that are not cast and contain an indirect association must be encrypted.

Discussion
Encryption of the ballot preserves the confidentiality of the voter's ballot selections while the ballot is tied to an indirect association to the voter.

Applies to: E2E voting system architectures
Related requirements: Data Protection

10.2.2 – Identification in vote records

10.2.2-A – Identifiers used for audits

Identifiers used for tying a cast vote record (CVR) and ballot images to physical paper ballots must be distinct from identifiers used for indirect associations.

Discussion
For the purpose of these requirements, associations between physical ballots and CVRs are not considered direct or indirect identifiers.

Related requirements: Auditability

10.2.2-B – No voter record order information

The voting system must not contain data or metadata associated with the CVR and ballot image files that can be used to determine the order in which votes are cast.

10.2.2-C – Identifying information in voter record file names

CVR and ballot image file names must not include any information identifying a voter.

Discussion
This helps to ensure that information that could accidently be used to reference a voter is not used within a file name.

10.2.2-D – Non-memorable identifiers and associations

Unique identifiers and associations must not be displayed in a way that is easily remembered by the voter.

Discussion
Unique identifiers on the paper record are displayed or formatted in such a way that they are not easily remembered by voters, such as by obscuring them in other characters.

Related requirements: 9.4 Efficiency

10.2.2-E – Aggregating and ordering

Aggregated and final totals:

1. must not contain voter specific information, and
2. must not be able to recreate the order in which the ballots were cast.

10.2.3 – Access to cast vote records (CVR)

10.2.3-A – Least privilege access to store

The directory or storage location of CVRs, ballot images, and ballot selections on the voting system must be subject to the principle of least privilege.

Discussion

NIST SP 800-12 defines "least privilege" as, "The security objective of granting users only those accesses they need to perform their official duties."

Nieles, Dempsey, and Pilliteri, *Special Publication (SP) 800-12 Revision 1, An Introduction to Information Security*, National Institute of Standards & Technology (NIST), Gaithersburg, Maryland, June, 2017.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

External references:	NIS SP800-12 Revision 1
Related requirements	Access Control

10.2.3-B – Limited access

Permission to access the directory or storage location for CVRs, ballot images, and ballot selections must be assigned to as few entities as possible.

Discussion

Entities include people and applications or processes running on the voting system.

Related requirements	Access Control

10.2.3-C – Authorized access

Permissions to access the directory or storage location for CVRs, ballot images, and ballot selections must be validated and explicitly authorized before access is given.

Discussion

Modern operating systems often have sufficient mechanisms in place to accomplish this, but these security capabilities need to be configured and enforced.

Related requirements	Access Control

10.2.3-D – Digital voter record access log

The voting system must log all access to the directory or storage location for CVRs, ballot images, and ballot selections in addition to logging access to all actions occurring within the system.

Discussion

This ensures that any person, process, or other entity reading, writing, or performing other actions to the electronic audit trail is properly logged.

Related requirements Access Control, Auditing

10.2.4 – Voter information in other devices and artifacts

10.2.4-A – Voting information in receipts

Receipts produced by a voting system must not contain voter information.

10.2.4-B – Ballot secrecy for receipts

The voting system must not issue a receipt to the voter that would provide proof to another of how the voter voted.

Applies to: E2E voting system architectures
Prior VVSG Source: 2007 Vol 1: 3.2.3.1-A.4

10.2.4-C – Logging of ballot selections

Logs and other portions of the audit trail must not contain individual or aggregate ballot selections.

Discussion
The voting system needs to be constructed so that the security of the system does not rely upon the secrecy of the event logs. It will be considered routine for event logs to be made available to election officials, and possibly even to the public, if election officials so desire. The system will be designed to permit the election officials to access event logs without fear of negative consequences to the security and integrity of the election. For example, cryptographic secret keys or passwords will not be logged in event log records.

10.2.4-D – Activation device records

Activation devices must not create or retain information that can be used to identify a voter's ballot, including the order and time at which a voter uses the voting system.

Discussion
Information such as the time the voter arrived at the polls or the specific vote-capture device used by the voter may be used to link a voter with their specific ballot and violates the principle of ballot secrecy.