Vanguard 1.0

System Use Specifications Version 1.0

Texas Secretary *of* State
Elections Division

800-252-VOTE • 512-463-5650
sos.texas.gov • votetexas.gov

Revised
3/31/2026

TABLE OF CONTENTS

1.0 SCOPE

The use specifications in this document govern the use of the Hart Verity Vanguard 1.0 voting system in elections conducted under the Texas Election Code. The document includes certain legal requirements and recommended best practices but is not intended to serve as a comprehensive user manual. These specifications must be applied in conjunction with all applicable statutory and administrative requirements. The Secretary of State may modify or clarify use requirements as necessary to ensure the effective and lawful conduct of an election.

2.0 SYSTEM DESCRIPTION

The Hart Vanguard 1.0 system is a voting system certified for use in Texas with software, hardware, device, and peripheral components designed to allow election officials to program an election, administer voting, and tabulate election results and to allow voters to mark and cast their ballots.

2.1 CERTIFIED COMPONENTS

2.1.1 Workstation (Election Management System)

- Vanguard Define: Election Data Management Application
- Vanguard Deploy: Election Definition Software Application
- Vanguard Capture: Central Scanning Software Application
- Vanguard Results: Tabulation and Reporting Software Application
- Vanguard Settings: Settings Adjustment Utility Module
- Vanguard Manage: Election Creation and Management Utility Module
- Vanguard Users: User Account Management Module
- Vanguard Libraries: Audio Files and Translation Module
- Vanguard Test Decks: Logic and Accuracy Test Deck Module

2.1.2 Devices (Voting System Units)

- Vanguard Flex: Ballot Marking Device
- Vanguard Vault: Precinct Scanner
- Vanguard Boost: Paper Ballots on Demand Device and Activation Device for Ballot Marking Devices

2.2 NON-CERTIFIED COMPONENTS

- Vanguard Ranked Choice Software Module
- Vanguard Adapt Device

2.3 SYSTEM CONFIGURATION

Entities may acquire and deploy individual components of the Hart Vanguard 1.0 voting system based on local election needs.

All Vanguard workstations installations include Vanguard Users, Vanguard Manage, and Vanguard Settings. Additional workstation and system components may be selected based on operational needs. System configuration and procurement decisions may also vary based on factors such as whether:

- The entity utilizes hand-marked paper ballots or deploys marking devices for all voters.
- Ballots are hand-counted or tabulated using tabulation components.
- Tabulation occurs at the precinct or through central counting.
- Ballot programming is conducted by the vendor or entity.

3.0 ACCEPTANCE TESTING

Acceptance Testing must be conducted in accordance with Section 129.021 of the Texas Election Code immediately upon delivery of a new voting system or new equipment components from the vendor.

3.1 VERIFICATION OF CERTIFICATION STATUS

Verify that the system delivered is certified by the Texas Secretary of State. To verify certification, compare the delivered system to the applicable certification order, including software name and software and/or firmware version(s).

3.2 HASH VALIDATION

Perform hash validation on each voting system unit. The Vanguard 1.0 system supports two methods for hash validation:

- System validation tool on voting system devices and workstations; and
- Manual retrieval of system files for direct hash validation.
    - **Manual method for hash validation may not be used for the Vanguard Workstations.**

Either method satisfies the hash validation requirements of Texas law for voting system devices. However, manual validation is an important method, as it provides an independent means of verification, but it requires greater technical knowledge and physical removal of the CFAST card from the voting device.

Each jurisdiction must determine which method to use. The Secretary of State recommends that jurisdictions consider using a combination of both methods over the lifecycle of the voting system devices.

3.3 HARDWARE DIAGNOSTICS TESTING

Perform a hardware diagnostic test on each voting system device included in the system. Hardware diagnostics testing ensures that all mechanical and electronic components are functioning properly. This testing will require a test election to be loaded using all functional configurations applicable to the jurisdiction.

A hardware diagnostic test must be performed on each voting system device included in the system. For guidance on executing testing requirements, refer to:

- Secretary of State Advisory No. 2019-23 – Electronic Voting System Procedures Advisory
- Vanguard Flex Device Support Guide, if applicable
- Vanguard Vault Device Support Guide, if applicable
- Vanguard Boost Device Support Guide, If applicable

When conducting hardware diagnostics testing, ensure the following components and peripherals are included in the test, as applicable:

- Autoballot (Barcode Scanner);
- Vanguard ATI (Accessible equipment), including access controller, headphones, sip and puff, and all other accessible input devices;
- VotePass functionality on the Vanguard Boost and Vanguard Flex; and
- Security tickets by opening and closing polls.

3.4 LOGIC AND ACCURACY TESTING (ACCEPTANCE TESTING)

Logic and accuracy testing must be conducted in accordance with Section 129.023 of the Texas Election Code. Additional guidance is available in Secretary of State Advisory No. 2019-23 – Electronic Voting System Procedures Advisory.

Note: Test decks generated by the system may be used only to supplement ballots produced by Vanguard Flex, Vanguard Boost, or other paper ballots the entity will utilize. Automatic adjudication may not be enabled to adjudicate ballots.

Hardware diagnostic and logic and accuracy testing for Acceptance Testing may be combined into a single testing activity, provided that all statutory requirements applicable to both acceptance testing and L&A testing are fully satisfied.

4.0 SECOND AND THIRD TABULATION TEST

A second tabulation test must be conducted immediately before the counting of ballots or accumulation of vote totals begin. A third tabulation test must be conducted after the counting of ballots or accumulation of vote totals has been completed. Both tests are required under Section 127.093 of the Texas Election Code. Refer to the Vanguard System Administrator's Guide for support concerning second and third testing in the system.

5.0 DEVICE USE SPECIFICATIONS

This section describes required settings, configuration, reports, and usage terms with the Vanguard system. It does not cover all available configurations which may vary by entity based on local needs and workflows.

5.1 VANGUARD VAULT

Refer to the Vanguard System Administrator's Guide, Vanguard Deploy User Guide, and Vanguard Vault User and Support Guides for general operational instructions for the Vanguard Vault.

5.1.1 Device Report Configuration

Deploy > Configure Settings > Election Settings > Device Reports	
Sort within a contest	By ballot order
Report results	Precinct
Zero Report	Precinct
Ballot Count Report	Precinct
Tally Report	Precinct
Number of Tally Reports	Three
Device Report Signature Text	"Election Judges and Poll Watchers"

5.1.2 Voting Type Configuration

Deploy > Configure Settings > Election Settings > Voting Type Setup			
	Allow Tally	**End Date and Time**	**End of Day Type**
Absentee	Yes	Election Date at 7 p.m.	Both
Early Voting	Yes	Election Date at 7 p.m.	Both
Election Day	Yes	Election Date at 7 p.m.	Close Polls

5.1.3 Ballot Scanning Behavior

Deploy > Configure Settings > Election Settings > Vault		
Mismark Type	**Scan Behavior**	**Override by (Voter or Poll Worker)**
Overvotes	Reject All	Voter
Overvotes	Reject All	Voter
Blank Ballot	Reject All	Voter
Invalid Votes	Reject All	Poll Worker
Blank Page	Reject All	Voter
Marginal Mark	Reject All	Poll Worker

Other Settings	**Scan Behavior**
Save scanned images on vDrive	Yes
Save scanned PVRs on vDrive	Yes
Enable Imprinting	Optional
Show summary screen after scan	Optional

5.1.4 Device Usage

- During Early Voting, the ballot scanner must be unplugged and sealed after voting hours.
- Precinct ballot counters used during early voting may not be used for voting on election day.
- The ballot box connected to a precinct ballot counter that is used during early voting by personal appearance must have two locks, each with a different key, and must be designed and constructed so that the box can be sealed to detect an unauthorized opening of the box.
- The general custodian of election records shall create a process and maintain a procedure for tracking the custody of the voting device equipment once the equipment is loaded with an election definition.

5.1.5 Vanguard Vault Reporting

- **Zero Report**—Required prior to polls opening on the first day of Early Voting and Election Day.
- **Open Polls Report**—Early Voting beginning of day ballot count to compare ballots cast to previous day's voter check-in totals.
- **Ballot Count Report**—Required at the end of voting on the last day of Early Voting.
- **Close Polls Report (Tally Report)**– Report automatically prints when polls are closed.
- **Audit Log**—Automatically loaded into Results when the V Drive is read; can also be exported to a thumb drive from the device.

5.2 VANGUARD CAPTURE

Refer to the Vanguard System Administrator's Guide and Vanguard Capture User Guide for general operational instructions for Vanguard Capture.

5.2.1 Capture Settings

Settings can be made in Election Preferences, which applies to all elections, or within the Settings menu of a specific election.

Ballot Resolution/ Automatic Acceptance	Yes/No
Undervotes	No (entities may sort and automatically accept contests with undervotes on PVRs in Vanguard Capture after batch scanning is complete)
Overvotes	No
Invalid Votes	No
Damaged Contests	No
Marginal Marks	No

5.2.2 Vanguard Capture Reporting

- **Zero Report (Configuration Report)**—Required prior to scanning ballots.
- **Batch Summary Report**—Required to record all the number of ballots exported to a vDrive. Ensure one Report per vDrive.
- **Audit Log Report**—All activity that has occurred in the Capture application on that workstation.
- **System Log Report**—All non-election specific activity on the workstation.

5.3 VANGUARD RESULTS

Refer to the Vanguard System Administrator's Guide and Vanguard Results User Guide for general operational instructions for Vanguard Results.

5.3.1 Reporting Options Configuration

Results > Reporting Options > Various Tabs	
Report Results	Precinct
Sort Contest Results	By Base Ballot Order
Report unassigned write-ins as	Separate Category
Report rejected write-ins as	Separate Category

5.3.2 Write-in Management

- Write-in candidate name alternate spelling is not permitted.
- Automatically accepting typed write-ins (for PVR ballots) is optional.

5.3.3 Vanguard Results Reporting

- **Zero Report (Cumulative Results Report)**—Required before any V-Drives are tabulated by the central accumulator.
- **Cumulative Results Report**—Include all voting types (Early Voting, Election Day, Ballot by Mail), undervotes, and overvotes.
- **Precinct Results Report**—Required after all ballots have been tabulated on election night, and again by Canvass.
- **Results Report by Polling Location**—Produce a Custom Report using the Cumulative Results Report and filter by Polling Place.

6.0 BALLOT NUMBERING AND UNIQUE IDENTIFIERS

Refer to the Vanguard Deploy User Guide and the Vanguard System Administrator's Guide for information concerning Ballot Numbering and Unique Identifiers.

6.1 UNIQUE IDENTIFIERS

The Hart Vanguard 1.0 system supports the use of non-serialized unique identifiers on ballots to prevent the scanning and tabulation of duplicate ballots. When enabled, the unique identifier:

- Is embedded within the ballot's validation barcode.

- May also be printed as a human-readable number in the ballot margin.

The Office of the Texas Secretary of State strongly recommends that entities utilize the system-generated unique identifier on both paper ballots and PVRs as an additional safeguard against duplicate ballot scanning.

6.2 UNIQUE IDENTIFIERS TO SATISFY BALLOT NUMBERING REQUIREMENTS

Entities may utilize the human-readable unique identifier to satisfy Texas ballot numbering requirements. Entities choosing this option must generate the Ballots Issued Report no later than 30 days after Election Day.

6.3 BALLOT NUMBERS

The Hart Vanguard 1.0 system supports the use of a sequential ballot number on paper ballots and PVRs. The use of system generated sequential ballot numbering is subject to the following limitations:

- Sequential ballot numbers may only be used to satisfy Texas ballot numbering requirements for paper ballots issued on-demand by the Boost system, or paper ballots generated by Vanguard Build for ballot by mail issuance or for ballots prepared for delivery to polling place locations.
    - Ballots delivered to the polling location must not be issued to voters in sequential order.
- Sequential ballot numbering must not be used for ballots issued by the Flex system or by the Vanguard Boost in the polling location due to voter privacy concerns.
- The ballots shall be tracked, distributed, and retained in accordance with Sections 51.006, 51.007, and 51.008 of the Texas Election Code.

6.4 COORDINATION WITH PRINTING SERVICES

If an entity uses system-generated unique identifiers or ballot numbering and also utilizes a separate ballot printing service, the entity must coordinate with all vendors involved to ensure that duplicate unique identifiers or ballot numbers are not produced.

7.0 AUDIT LOGS

After the automatic counting of ballots during central counting station is complete, the manager of the central counting station must produce a copy of the audit log to retain with other election records. The Verity Vanguard 1.0 workstation allows the user to export all workstation logs to a single file named “Veritylogs.zip” onto USB media. Refer to the Vanguard System Administrator’s Guide for more information.

8.0 SECURITY SEALS

Entities must apply and record seals in accordance with Section 123.034 of the Texas Election Code to prevent unauthorized access of equipment, including all device tamper-evident seal locations identified on the voting system units in the Security and Best Practices section of the Vanguard System Administrator's Guide.

9.0 MULTI-FACTOR AUTHENTICATION (MFA) DEVICE AND REMOVABLE MEDIA MANAGEMENT

9.1 CHAIN OF CUSTODY

The following requirements and recommendations cover the use management of multi-factor and removal media devices used in the Vanguard 1.0 system, including:

- Workstation Security Tokens;
- Verity Keys;
- Security Tickets;
- VotePasses;
- vDrives; and
- COTS Removal USB Media.

Jurisdictions must implement chain of custody procedures that follow vendor provided standards in the Security and Best Practices section of the Vanguard System Administrator's Guide and requirements of Section 123.034 of the Texas Election Code by:

- Logging all MFA devices and removable media inventory before and during an election.
- Ensuring that all MFA devices and removable media deployed during an election are accounted for and inventoried at the conclusion of the election.
- Following the Principle of Least Privilege when creating or issuing devices and aim to create only the minimum number of devices required to conduct the election.

Devices should be securely stored or assigned to a specific individual with documented custody.

9.2 WORKSTATION SECURITY TOKENS

Refer to the Vanguard System Administrator's Guide for information on Vanguard Workstation Security Tokens. Entities must:

- Adhere to the vendor's recommended security best practices provided on pages in the Vanguard System Administrator's Guide.
- Ensure Workstation Security Tokens and passwords are unique/user specific and not shared with others.
- Follow the vendor provided recommendations in the Vanguard System Administrator's Guide if a Workstation Security Token is lost or compromised.

Entities should document when an individual has been issued a Workstation Security Token and maintain inventory records in a similar manner to the entities' existing procedures when issuing items such as facility keys, access badges, and technology devices. Security Tokens should also be labeled with consistent naming convention for ease of identification, accounting, and inventory.

9.3 VERITY KEYS

Entities must adhere to the vendor standards in the Vanguard Deploy User Guide and the Vanguard System Administrator's Guide by:

- Limiting the number of keys generated.
- Maintaining chain of custody logs and limiting access to keys.
- Removing keys from equipment and store in a secure manner when not in use.
- Limiting access to Verity Key passcodes.
- Labeling keys using a consistent naming convention.
- Ensuring passcodes are unique to an election.
- Maintaining at least one backup Verity Key.

9.4 SECURITY TICKETS

Entities must adhere to the vendor security practices in the Vanguard System Administrator's Guide by ensuring that they:

- Never write or attach passcodes on Security Tickets.
- Prohibit users never share Security Tickets or passcodes with other individuals.
- Maintain unique passcodes across all different user levels.
- Update user credentials if a Security Ticket is lost.
- Import or export a Credential List on all affected devices after personnel changes.

9.5 VOTEPASSES

Jurisdictions using VotePass activation must follow vendor procedures in the Vanguard Boost Polling Place Guide and the Vanguard System Administrator's Guide by:

- Issuing a VotePass only after the voter has been qualified and a voting booth is available.
- Never issuing VotePasses in bulk.
- Handling spoiled ballots in accordance with the Texas Election Code.

Jurisdictions should consider a collection method near voting booths or the polling place exit for voided VotePasses. Discarding the voided VotePasses as waste is strongly discouraged.

9.6 VDRIVES (USB)

Entities must adhere to the vendor security practices in the Vanguard System Administrator's Guide and Vanguard Deploy User Guide when generating and deploying vDrives by:

- Restricting vDrive creation to authorized personnel only following the Principle of Least Privilege.
- Labeling vDrives with a consistent naming convention that is easily identifiable for their designated location at the time of loading.
- Maintaining chain of custody when transporting and receiving vDrives.
- Retaining all vDrives containing election data for the statutory retention period.

- Accounting for unused vDrives (e.g., spares, emergency backups, or training units) by ensuring they are properly labeled and either securely stored or immediately cleared and reformatted for future use.
- Exporting Log Data and Temporary Logs from the Vanguard device to a COTS USB if a Recovery vDrive is required.

9.7 COTS REMOVABLE MEDIA (USB)

Entities must adhere to the vendor provided standards in the Vanguard System Administrator's Guide concerning the use of COTS removable media by doing the following:

- Implement a general Removal Media Policy.
- Use only new or reformatted COTS removable media when transferring data between Vanguard components and non-Vanguard component.
- Clear and re-reformat used COTS removable media between elections.
- Use NTFS Formatting standard for COTS USB media.
- Retain COTS removable media containing election data for the statutory retention period.

Entities should only use COTS removable media that has been purchased new from a known and trusted source. Additionally, COTS removable media purchased to be used with the voting system should only be used for the voting system and election purposes. Jurisdictions should consider discontinuing the use of specific COTS removable media with the voting system if there are any security concerns related to the loss of chain-of-custody.

10.0 CERTIFICATE SETS (DIGITAL FILES)

Entities may request a jurisdiction-specific certificate set. If a jurisdiction-specific certificate set is acquired, the new certificate set must be updated on every Vanguard Workstation and device in the jurisdiction's inventory.

New certificate sets can only be created by the vendor and can only be stored on Certificate Keys. Notify the Election Technology and Security team within the Elections Division of the Texas Secretary of State if you will be requesting a jurisdiction-specific certificate set.

Jurisdictions that have any mutual aid agreements with other jurisdictions, including the loaning or renting of surplus equipment for emergencies, should consider these existing agreements prior to requesting a jurisdiction-specific certificate set.