ClearVote 2.3

ClearAccess Functionality Description

ClearAccess Functionality Description

Clear Ballot Part Number: 100049-10020

Document Type: Technical

Clear Ballot Group
2 Oliver Street, Suite 200
Boston, MA 02109
857-250-4961
clearballot.com

Document history

Date	Description	Version	Authors
01/11/2017	Initial submission to EA	1.0	Nel Finberg
02/03/2017	Minor typographical and reference-related edits.	1.0.1	Nel Finberg
05/15/2017	Minor edits.	1.0.2	Nel Finberg
06/16/2017	Minor updates for vote-by-mail campaign.	1.0.3	Joni McNutt
07/20/2017	Data retention section revised to point to election archiving procedure in ClearAccess Supervisor Guide. Reference to work plan in ClearAccess Supervisor Guide added to Ballot and program installation and control section. Narrative complying with Post-voting capabilities requirements provided.	1.1	Nel Finberg
09/26/2017	Execution of intended/necessary processes revised. Reference to voting screen specifications provided in Paper-based system requirements.	1.2	Nel Finberg
10/19/2017	Minor edits.	1.2.1	Nel Finberg
10/31/2017	Revised Marksense systems.	1.3	Nel Finberg
11/02/2017	Revised Ballot Production.	1.4	Nel Finberg
11/03/2017	Ballot Production revised to point to paper stock used in certification testing. Maintenance, transportation, and storage revised to point to original manufacturer packaging for transport.	1.5	Nel Finberg
01/19/2018	Vote-by-Mail campaign 2	1.5.1	Joni McNutt
04/27/2018	Sections renumbered to use new numbering scheme. Minor edits.	1.5.2	Mike Quigley
04/12/2019	Added BDF, ballot image, and results file encryption. Minor edits.	1.5.3	Mike Quigley
11/22/2019	Updated headings and minor edits.	1.5.4	Joe Srednicki
02/12/2020	Minor edits.	1.5.5	Joe Srednicki

Date	Description	Version	Authors
12/09/2020	Minor edits.	1.5.6	George Petta
09/20/2021	Minor edits.	1.5.7	Eric Burz

Table of contents

Preface

This section defines the purpose of this document.

About this document

This document provides a functional description of the ClearAccess accessible voting system. It complies with the documentation requirements of Voluntary Voting System Guidelines (VVSG) Volume I, 2 Functional Requirements and *Volume II, 2.3 System Functionality Description*.

Scope of this document

This document contains the following chapters:

- Chapter 1. Functional requirements
- Chapter 2. System functionality description

Intended audience

The document is for state and federal election officials and their voting system test laboratories. This document is part of the Technical Data Package (TDP) required to certify the ClearVote system for use. Clear Ballot personnel also use this document to support election officials and staff.

Conventions

This section describes conventions used in this document.

References to ClearVote products

A ClearVote® system can comprise the ClearAccess®, ClearCast®, ClearCount®, and ClearDesign® products. Jurisdictions are not required to purchase all products. You can ignore references to any ClearVote products that are not part of your voting system. Also ignore implementation options that are not relevant to your policies and procedures.

BDF and ADF

ClearAccess imports an election definition contained in an accessible definition file (ADF) created by ClearDesign. ClearCount and ClearCast import an election definition contained in a ballot definition file (BDF) created by ClearDesign.

Versions of ClearDesign earlier than 2.0 created unencrypted ADFs and BDFs. ClearDesign 2.0 and later versions produce encrypted ADFs and BDFs. You can distinguish between unencrypted and encrypted ADFs and BDFs by the ending of the filename.

File type	Filename ends in
Unencrypted accessible definition file	adf.zip
Encrypted accessible definition file	adfx.zip
Unencrypted ballot definition file	bdf.zip
Encrypted ballot definition file	bdfx.zip

In this document, the general terms ADF and BDF can refer to both the unencrypted and encrypted versions of these files.

For the specifics of the ADF and BDF file formats, see the following:

- *ClearDesign Accessible Definition File Guide*
- *ClearDesign Ballot Definition File Guide*

Chapter 1. Functional requirements

This chapter describes the functional requirements for ClearAccess.

1.1 Overall system capabilities

1.1.1 Security

ClearAccess security consists of the following:

- Programmatic access control established by codes and user access levels
- Data encryption
- Physical security

The ClearAccess system architecture and recommended procedures work together to ensure security.

Access controls

The ClearAccess system has five roles (Table 1-1) that control access to the system. Each role has its own code.

Table 1-1. ClearAccess roles

Role	Allows
Maintenance	Service and maintenance personnel to set up and maintain the device. This role has no access to any election data.
Administrator	Device administrators to set up the system, define device codes, and load and unload elections. This role has no access to any voting activity.
Election Administrator	Election administrators to validate the election, perform election pretesting, such as Logic and Accuracy testing (LAT), and prepare the device for the election.
Poll Worker	Poll workers to open and close the polls.
Voter	A poll worker to activate a voting session and select the precinct and ballot for the voter. Once poll worker selects the ballot, the voter can vote independently.

Process control

Internal controls ensure that functions and tasks execute in ClearAccess only under the intended conditions. For example, ClearAccess does not allow a voting session to begin until the polls are open.

Precondition control

Internal controls ensure that functions and tasks execute in ClearAccess only after meeting the required preconditions. Example are:

- ClearAccess does not allow users to access the system until they log in by selecting a role and entering a code.
- ClearAccess cannot load the accessible definition file until a user enters the correct code. Codes are specific to individual elections.
- A voting session cannot begin until the polls are open.

Safeguards if a system failure occurs

To prevent tampering during system repairs or interventions in system operations, the ClearAccess system limits the functionality of the Maintenance user.

The only election data stored on the system is the election definition contained in the accessible definition file. ClearAccess validates the election definition when the accessible definition file is loaded and each time the system starts.

Security provisions

The *ClearVote Security Policy* describes safeguards for preparing, testing, and operating the voting equipment.

Restricted access

Permissions associated with roles control access to system capabilities. See "Access controls" on the previous page. The state of an election also determines when a user can perform functions associated with an assigned role.

Procedural controls used in a jurisdiction can restrict unauthorized access to the system.

Mandatory administrative procedures

The *ClearVote Security Policy* documents mandatory administrative procedures for effective system security.

1.1.2 Accuracy

Record elections accurately

An election is defined in ClearDesign, which uses the election code to create an HMAC of the election data. When an administrator loads an accessible definition file (ADF or ADFx) into ClearAccess, the administrator is prompted for an election code. ClearAccess validates the election code before loading the accessible definition file.

An ADFx is encrypted by using AES256-CBC technology. Encryption ensures that only ClearDesign can change the election data in an ADFx and only ClearAccess can read this data.

Options for casting and recording votes

Options for casting and recording votes are configured in ClearDesign.

Record votes precisely

ClearAccess captures votes and records them accurately on a printed ballot. The system does not retain vote selections. ClearAccess does not count or tally ballots.

Control logic and data processing methods

The ClearAccess ballot-marking device provides a Ballot Report. This report includes counts of all voting sessions, ballots printed, re-printed, or canceled, by precinct, split, and ballot type, with corresponding totals. The Ballot Report can be issued in either Pre-election or Election mode. The report does not contain any vote-tally information.

Monitor overall data quality

ClearAccess validates an accessible definition file by using an HMAC. This validation process ensures that the accessible definition file is unaltered.

Accurate recording, tabulating, and recording of votes

This requirement does not apply to ClearAccess because it is not a DRE.

1.1.3 Error recovery

Device restoration

When an error occurs, ClearAccess restores the system to the operating condition immediately before the error or failure.

ClearAccess validates all data before attempting to update the system. The user is informed of any error or inconsistency and can correct it before updating the system.

Any anomalous condition that can occur while voting a ballot has a straightforward resolution. Such conditions include:

- Overvoting
- Undervoting
- Blank voting

To resolve these conditions, see "Error Messages" in the *ClearAccess Supervisor Guide*.

The device does not store any vote-tally information. If the ClearAccess device fails during a voting session, the voter can be issued a new ballot.

Resumption of normal operation

The only election data stored on the system is the static accessible definition file that was generated by ClearDesign. If a system failure occurs, an administrator can reload the accessible definition file from the original media. ClearAccess does not store any information about cast ballots or vote tallies.

If a device failure occurs, an administrator can load the accessible definition file into an alternate ClearAccess device. If the failure occurred while voting, a jurisdiction can offer the voter an alternate ClearAccess device for voting.

Recovery from external conditions

The following practices minimize the effect of and ensure recovery from external conditions:

- ClearAccess software runs on COTS hardware. If a device becomes damaged or fails, another standby device can be easily swapped in.
- Clear Ballot recommends performing preventive maintenance as described in the *ClearAccess Maintenance Guide*.

1.1.4 Integrity

Protection against a single point of failure

Following the procedures in the *ClearAccess Maintenance Guide* prevents a single point of failure at the polling place.

Protection against the interruption of electrical power

The computers supported by ClearAccess do not include internal batteries. The computers can use a UPS to ensure continued accessible voting if a power failure occurs.

Protection against generated or induced electromagnetic radiation

ClearAccess uses COTS hardware. The manufacturers have developed and testing this hardware to protect against physical threats such as generated or induced electromagnetic radiation.

Protection against ambient temperature and humidity fluctuations

Jurisdictions must store and operate the ClearAccess system within the temperature and humidity tolerances stated in the ClearVote TDP submission.

Protection of the data input or storage device from failure

Following the procedures in the *ClearAccess Maintenance Guide* protects the data storage and input devices from failure.

If the core memory in the ClearAccess station fails, replace the station. In this situation, the voter may be required to vote again.

Protection against improper data entry and retrieval

The ClearAccess application validates all data entry and accepts only properly validated data. This guideline does not apply to data input from predefined choices, such as menu buttons.

A user can access only the functionality and information allowed by his or her assigned role and the current status of the election.

When using ClearAccess, a voter can access only the eligible contests, candidates, and measures that are available on the voter's ballot.

The ClearAccess application does not store any vote-tally information.

When a user logs in, ClearAccess validates the accessible definition file by using an HMAC. If the validation process detects any unauthorized alteration of data, ClearAccess does not load the election.

An ADFx is encrypted by using AES256-CBC technology. Encryption ensures that only ClearDesign can change the election data in an ADFx and only ClearAccess can read this data.

Date and time of normal and abnormal events

ClearAccess records all user interactions and the date and time of the event in a log. Authorized personnel can view and print logs.

Permanent record of audit data

ClearAccess maintains a permanent log of all audit data. Users cannot edit, change, or overwrite log data. Audit logs are updated only by the automatic recording of system- or election-related events.

The count of ballots printed increments during the voting period of an election. ClearAccess produces paper ballots that can then be voted by inserting them into a ballot-counting device.

Detection and recording of events

ClearAccess records every event in the pertinent system or election audit logs, including any potential error conditions that the system cannot overcome.

No time-dependent or programmed events occur in the ClearAccess accessible voting system.

Built-in measurement, self-test, and diagnostics

The Windows operating system automatically verifies system operation when the Clear station is turned on.

The logic and accuracy test (LAT) performed on the ClearAccess system before an election exhaustively verifies system functionality.

Redundant ballot storage

This requirement does not apply to the ClearAccess because it is not a DRE.

Retention of human-readable ballot images

This requirement does not apply to ClearAccess because it is not a DRE.

1.1.5 Operational requirements for system audit

The following topics describe some operational requirements for auditing the system:

- "Timing and sequences of audit records" below
- "Error messages" on page 16
- "Status messages" on page 16
- "Use of shared computing platforms" on page 17

1.1.6 Timing and sequences of audit records

The following topics describe the timing and sequence of audit records.

Real-time audit record

The ClearAccess system has two types of audit logs:

- System log
- Error log

ClearAccess records error conditions in the appropriate log. Log entries do not contain any information about specific voters or voted ballots.

ClearAccess stores the system log and election log in permanent files to preserve their integrity. ClearAccess logs events whenever the system operates. System activity does not affect the integrity of the logs.

Users can view and print the audit logs in any election mode.

A user identifies an error condition when a message appears on the screen. Users can analyze error conditions by reviewing the logs, if necessary.

For more information, see "Logs" in the *ClearAccess Supervisor Guide*.

Real-time clock

The ClearAccess software runs on a COTS computer that contains a real-time clock.

Time-and-date stamp

Every audit log entry contains a time-and-date stamp.

Operating mode

ClearAccess auditing functionality is active whenever the system is operational.

Termination of audit recorded entries

The ClearAccess application and users cannot stop the recording of log entries or alter them. Clear always maintains the physical security and integrity of the logs.

The ClearAccess application runs in kiosk mode. The logs are available in read-only mode in the ClearAccess user interface.

Preservation of contents

The contents of the audit logs are preserved when a power failure occurs.

Printing

Users can print the ClearAccess logs. Printing a log does not interfere with the production of any output reports.

Each log entry contains the following information:

- Timestamp – the date and time the event occurred
- Severity – the identifier of severity of the event
- User – the user associated with the event. There is no user for failed login attempts.
- Message – the message describing the event

Log entries are kept physically secure by using a block chaining and hashing mechanism. See "ClearAccess Security Specifications" in the *ClearAccess Security Specification*.

1.1.7 Error messages

Generation, storage and reporting

The ClearAccess voting system generates and reports error messages to users and posts corresponding entries in the audit logs as events occur. See "Error Messages" in the *ClearAccess Supervisor Guide*.

Easily understood text

All error messages requiring intervention by an operator or precinct official appear in easy-to-understand text.

Numerical error codes

The ClearAccess system does not use numerical codes to identify errors.

Understandable error messages

Elections officials can easily understand all error messages after receiving training on using and operating the system.

Message cues

Messages clearly state the required action when a voter or operator response is required.

Erroneous responses

An erroneous response to an error condition does not result in an irreversible error.

Nested error conditions

ClearAccess corrects nested error conditions in a controlled sequence. ClearAccess returns the voting system to the state before the first error occurred.

Status messages

ClearAccess displays status information in real time.

ClearAccess displays and reports critical status messages by using clear indicators or English language text. ClearAccess does not use numerical codes in status messages.

Status messages are posted to the appropriate audit log. Jurisdictions can designate which messages are critical.

1.1.8 Use of shared computing platforms

Authentication

The ClearAccess station is configured to provide the required Windows authentication. See "Hardening the ClearAccess Station" in the *ClearAccess Installation Guide*.

Operating system audit

The Windows Event Viewer is always active when ClearAccess is in use.

The Windows Event Viewer audits event related to the operating system, including:

- The opening and closing of all sessions and connections
- All process executions and terminations
- The alteration or deletions of any memory or file object

To reach the Windows Event Viewer, click the Windows icon on the left of the status bar at the bottom of screen and type **Event Viewer**.

Execution of intended and necessary processes

The hardening process ensures that only the intended and necessary processes execute while ClearAccess is running. For a description of hardening, see the *ClearAccess Installation Guide*.

In its hardened state, the ClearAccess station operates in kiosk mode. In this mode, only the ClearAccess application and nominal operating system components run on the ClearAccess station.

The ClearAccess software becomes inoperable when any critical system process, such as auditing, terminates.

1.1.9 Election management system

The ClearDesign election management system provides the election and ballot content used to configure the ClearAccess system for an election. ClearDesign writes the election and ballot information to an accessible definition file. An administrator then loads the accessible definition file for an election into ClearAccess.

Before every election, perform logic and accuracy testing (LAT) to ensure that ClearAccess will operate as intended.

After an election closes, officials can review reports on ballot-printing statistics.

Users can view and print audit reports when ClearAccess is any election state.

1.1.10 Vote tabulating program

Functions

The requirements of this section do not apply to the ClearAccess ballot marking device because it is not used to tabulate votes.

Voting variations

The ClearAccess accessible voting system supports the use of:

- Closed primaries
- Open primaries
- Partisan offices
- Nonpartisan offices
- Write-in voting
- Primary presidential delegation nominations
- Ballot rotation
- Straight-party voting
- Cross-party endorsement
- Split precincts
- Vote for N of M
- Recall issues with options
- Provisional or challenged ballots

ClearAccess currently does not support:

- Cumulative voting
- Ranked order voting

1.1.11 Ballot counter

The ClearAccess ballot-marking device provides a Ballot Report. This report includes counts of all voting sessions, ballots printed, re-printed, or canceled, by precinct, split and ballot type, with corresponding totals. The Ballot Report can be issued in either Pre-election or Election mode.

The Ballot Report does not contain any vote-tally information. ClearAccess does tabulate ballots.

1.1.12 Telecommunications

This requirement does not apply to ClearAccess because it is never connected to a telecommunications network.

1.1.13 Data retention

See "Archiving election materials" in the *ClearAccess Supervisor Guide*.

1.2 Pre-voting capabilities

1.2.1 General capabilities for ballot preparation

ClearDesign is used to set up elections and ballots. ClearAccess is not used for ballot preparation.

1.2.2 Ballot formatting

Newly defined elections

ClearDesign defines elections and ballot layouts. This requirement does not apply to ClearAccess because it does not define elections and ballot layouts.

Definition of elections

ClearDesign defines elections and ballot layouts. This requirement does not apply to ClearAccess because it does not define elections and ballot layouts.

Uniform allocation of space and fonts

ClearAccess formats each office, candidate, and contest on the ballot so that no voting position appears preferable to any other.

ClearAccess overrides font-size variations to allow for a uniform appearance across candidates unless subheaders are used. Subheaders allow for the use of multiple font sizes within an individual entry. Subheaders are normally applied uniformly across candidates to achieve a consistent appearance on the ballot.

ClearAccess accurately displays bold, italic, and underline formatting. Any of these format options can be modified in ClearDesign.

Long candidate names require additional rows per candidate. When set up in ClearDesign, these additional rows appear on the ClearAccess ballot. Additional rows appear consistently for all candidates in each contest.

Each page of the ClearAccess visual ballot contains a single contest. If the list of candidates displayed exceeds the visible page, the voter can scroll through the list.

Voting positions appear in a consistent size, shape, and position on the ballot.

Simultaneous display of choices

All choices in a single contest are displayed on the ClearAccess visual ballot simultaneously.

Format retention

A jurisdiction must ensure that previously defined ballot formats in accessible definitions files are retained as required.

Unauthorized modification

See "Validation" in the *ClearAccess Security Specification*.

1.2.3 Ballot production

Ballot display

ClearAccess displays ballot contents on the touchscreen. The system prints the voter's ballot after it has been voted.

Languages

ClearAccess can display and print a ballot in any language required by the Voting Rights Act of 1965.

Advertising and commercial logos

By default, the ClearAccess user interface does not present any advertising or commercial logos of any kind, either directly or by hyperlink. A jurisdiction must prepare ballot content that complies with this requirement.

Paper stock

The stock on which ClearAccess ballots is printed must conform to the 90 lb. stock used for certification testing and the dimensions required by the election configuration.

Marksense systems

The stock on which ClearAccess ballots is printed must conform to the requirements of the printing device and the dimensions required by the election configuration.

Ballot format modification

ClearAccess uses an HMAC to validate an accessible definition file. If ClearAccess detects an unauthorized modification, it will not the load the election defined in the accessible definition file.

The ClearAccess user interface does allow any changes to the accessible definition file.

ClearDesign encrypts an ADFx by using AES256-CBC technology. Encryption prevents unauthorized access to the contents of the ADFx by applications other than ClearDesign and ClearAccess.

1.2.4 Election programming

After a ballot designer finalizes election and ballot content in ClearDesign, he or she generates the accessible definition file. An administration can then load the accessible definition file into ClearAccess.

The accessible definition file contains ballot content and voting options for the election, including any audio content for accessible voting. The same accessible definition file gets loaded into all ClearAccess units. Once the accessible definition file has been loaded into the ClearAccess station, an administrator can configure the vote center. The configured vote center limits the ballot content in the accessible definition file to the ballot styles required by the precincts at the voting location.

1.2.5 Ballot and program installation and control

Detailed work plan

To install the application, see the *ClearAccess Installation Guide*.

To set up an election, see "Loading an Election" in the *ClearAccess Supervisor Guide*.

Verifying software selection and installation

See the *ClearAccess Acceptance Test Checklist*.

Software matches ballot formats

The validation of ballot formats in the ClearAccess takes place during pre-election logic and accuracy testing (LAT). See "Pre-election testing" in the *ClearAccess Supervisor Guide*.

1.2.6 Readiness testing

Verifying the preparation for an election

Before an election, each ClearAccess station requires preventive maintenance. See "Preventive maintenance" in the *ClearAccess Maintenance Guide*.

Clear Ballot recommends documenting each task and archiving the documentation at the end of the election.

The presentation of the Voting Login screen when the polls have opened at the beginning of official voting demonstrates that the ClearAccess station is ready for voting.

Status and data reports

To prepare for the start of voting, an election administrator sets the ClearAccess station to Polls Open mode. When the election administrator sets Polls Open mode, the Open Polls report automatically displays on the ClearAccess station. The election administrator can verify the contents of this report to determine that voting can begin.

See "Opening the polls" in the *ClearAccess Supervisor Guide*.

Verifying the installation and interface

Table 1-2 lists some verification steps for the installation and interface.

Table 1-2. Verification steps

Verification	Indicates success in
The ClearAccess application launches.	Installing the ClearAccess application
ClearAccess enables you to open the desired election.	Loading the accessible definition file
The Voting Login screen appears after the polls have opened.	Preparing the ClearAccess station for voting

Verifying that the hardware and software function correctly

A jurisdiction must perform an acceptance test after receiving the equipment from the vendor. The acceptance test demonstrates that the voting equipment functions correctly.

See the *ClearAccess Acceptance Test Checklist*.

After the polls have opened, the appearance of the Voting Login screen indicates that the ClearAccess station is ready for voting.

Consolidated data reports

ClearAccess Ballot Reports can be reviewed and printed at the conclusion of equipment readiness testing.

Segregate test data

A jurisdiction must segregate test data procedurally.

Ballot and program installation

See the following:

- *ClearAccess Installation Guide*
- "Loading an Election" in the *ClearAccess Supervisor Guide*

Testing separately

No external software or hardware is used to simulate operator or voter functions.

Residual effect

No external software or hardware is used to simulate operator or voter functions.

Conversion testing—all potential ballot positions

This requirement does not apply to ClearAccess because it is not used to scan and count ballots.

Conversion testing—active position density

This requirement does not apply to ClearAccess because it is not used to scan and count ballots.

1.2.7 Verification at the polling place

Before voting begins, an official can print the Ballot Report. This report includes counts of all voting sessions, ballots printed, re-printed or canceled, by precinct, split and ballot type, with corresponding totals. The Ballot can be issued in either Pre-election or Election mode. This report does not contain any vote-tally information.

At the outset of the election, all official voting ballot counts are zero.

The report contains the name of the election and applicable polling place. The report contains information pertaining to an individual ClearAccess station.

Because the system does not maintain active candidate and measure registers, the report does not contain this information.

The appearance of the Voting Login screen at the beginning of official voting confirms the following:

- No hardware or software failures have occurred.
- The ClearAccess station is ready to be activated for accepting votes.

1.2.8 Verification at the central location

This requirement does not apply to ClearAccess.

1.3 Voting capabilities

1.3.1 Opening the polls: precinct count systems

This requirement does not apply to ClearAccess because it is not a precinct-count system.

1.3.2 Opening the polls: paper-based systems

Verifying preparation

The ClearAccess station is ready to use when a poll worker sees the Voting Login screen. See the poll opening procedures in the *ClearAccess Poll Worker Guide*.

Voting booth

The ClearAccess station is intended for use with a voting screen. The ClearVote TDP submission provides specifications for the voting screen.

Secure receptacle

A jurisdiction must place voted ballots in secure receptacles.

Activating device

This requirement does not apply to ClearAccess because it is not a precinct-count system.

Verifying activation

This requirement does not apply to ClearAccess because it is not a precinct-count system.

Identifying device failure

This requirement does not apply to ClearAccess because it is not a precinct-count system.

1.3.3 DRE system requirements

This requirement does not apply to ClearAccess because it is not a DRE.

1.3.4 Activating the ballot (DRE systems)

This requirement does not apply to ClearAccess because it is not a DRE.

1.3.5 Casting a ballot: common requirements

Three-millimeter-high text

ClearAccess can display ballot text at least three millimeters high. ClearAccess can adjust or magnify the text to a size of 6.3 millimeters.

Individual vote choices

ClearAccess records the selections of individual vote choices for each contest and ballot measure on a printed ballot but does not retain these selections in memory.

Voter secrecy

Clear Ballot does not maintain any information that identifies a voter. The voted ballot does not contain any identifying information.

A jurisdiction must ensure privacy when a voter marks a ballot and carries it to the counting device or secure ballot receptacle.

Write-ins

ClearAccess allows a voter to enter write-in candidates whose names do not appear on the ballot. A voter can enter as many write-in choices as the maximum number of allowed choices for a contest.

Power failure

The computers and printers supported by ClearAccess do not include internal batteries. A jurisdiction must provide UPS units at polling locations for backup power if a power failure occurs.

Telecommunications failure

This requirement does not apply to ClearAccess because it is never connected to a telecommunications network.

1.3.6 Casting a ballot: paper-based systems

Voting field

Voting fields on the touchscreen clearly identify the responses corresponding to contests and ballot measures.

Mark ballot

Voters can select candidates or responses to ballot measures by using the touchscreen, keypad, or sip-and-puff device. Voters can select up to the maximum number of allowed choices for each contest or ballot measure.

Casting ballot

After voting, the voter or election official must place the ballot in a secure receptacle or ballot-counting device.

Secrecy

The ClearAccess system and the voted ballot do not store or contain any information that identifies a voter.

The jurisdiction must ensure privacy when voters fill out ballots and then transport the voted ballots to a ballot-counting device or secure receptacle.

Undervotes

ClearAccess can be configured to identify undervoted and blank-voted contests before a voter completes the ballot.

Overvoted contest

ClearAccess does not allow overvoted contests.

Overvoted ballot

ClearAccess does not allow overvoted ballots.

Correcting undervotes and overvotes

The voter can correct an undervoted ballot before it is cast and counted. ClearAccess flags undervoted contests in the ballot review stage.

ClearAccess flags all overvoted contests and prevents a voter from casting ballots containing overvoted contests.

1.3.7 DRE system requirements

This requirement does not apply ClearAccess because it is not a DRE.

1.4 Post-voting capabilities

1.4.1 Closing the polls

Preventing further ballot casting

At the end of the election day, the polls are closed on the ClearAccess voting system. See "Closing the polls" in the *ClearAccess Supervisor Guide*.

Internal test

The Close Polls report displays automatically when the polls close. When this report contains the expected information, it indicates that officials have followed the prescribed closing procedure and that the status of the device is normal.

System status

The Close Polls report indicates system status.

Diagnostic test record

The display of the Close Polls report verifies appropriate the sequence of events.

The extraction of voting data does not apply to ClearAccess because it is not used to cast ballots.

Precluding unauthorized polls reopening

Poll workers must follow the established procedure for closing the polls in the ClearAccess system. Poll workers must ensure that polls are not reopened after they have been closed.

1.4.2 Consolidating vote data

This requirement does not apply to ClearAccess because it is not used to cast ballots.

1.4.3 Producing reports

The Close Polls report indicates the number of ballots printed, reprinted, and canceled in the voting session.

ClearAccess is not used to cast ballots. ClearAccess does not accumulate vote totals or produce reports containing election results.

Officials can view and print audit reports after the polls have closed and the system is in Postelection mode.

Generating reports does not alter or destroy any data stored on the system.

1.4.4 Broadcasting results

ClearAccess is not used to make unofficial results available to external organizations.

1.5 Maintenance, transportation, and storage

ClearAccess equipment will not degrade by moving to and from the place of use. ClearAccess equipment will not degrade when stored between elections if the jurisdiction uses the appropriate packaging and transport containers.

Use the original packing from the manufacturer when moving the ClearAccess station, personal assistive devices, and printer.

Chapter 2. System functionality description

This chapter describes system functionality.

2.1 Scope

ClearAccess enables physically-challenged people to vote comfortably, privately, and intuitively. Voters can view or listen to ballot content in the designated languages. Voters can then make ballot selections by using the touchscreen, numeric keypad, or sip-and-puff device.

ClearAccess is used to mark and print voted ballots but does not count or tally the ballots. ClearDesign is used to define the election and lay out ballots. ClearDesign writes the election definition and ballot layouts to an accessible definition file that gets loaded into ClearAccess.

2.2 Functional processing capabilities

For description of the functional capabilities of ClearAccess, see "Operations concept" in the *ClearAccess System Overview*.

2.3 Presentation of required capabilities

For a description of the functional capabilities of ClearAccess corresponding to *VVSG Volume I, Section 2*, see Chapter 1, "Functional requirements" on page 9.

2.4 Additional capabilities

All ClearAccess functionality is described in this document and the *ClearAccess Supervisor Guide*.

2.5 Bypassed and deactivated capabilities

The installation process for ClearAccess does not allow for the bypass or deactivation of any system capabilities.

2.6 Installing ClearAccess and activating capabilities

The installation process for ClearAccess automatically activates all system capabilities.

The functionality available to a user depends on the user's role and the current state of the election. For information on roles, see the following:

- "Access controls" on page 9
- "ClearAccess roles" and "ClearAccess election modes" in the *ClearAccess Supervisor Guide*

2.7 Installing and deactivating capabilities

The installation process for ClearAccess cannot bypass or deactivate any system capabilities. Also see the previous section.