Clear Ballot

ClearVote 1.5

Security Policy

ClearVote Security Policy

Clear Ballot Part Number: 100086-10013

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 EAC	1.0	Nel Finberg
02/03/2017	Minor typographical and reference-related edits	1.0.1	Nel Finberg
03/30/2017	Minor typographical and reference-related edits based on feedback from the State of Colorado	1.0.2	Joni G. McNutt
04/28/2017	Minor updates based on feedback from the State of Colorado and Clear Ballot Quality Assurance	1.0.3	Joni G. McNutt
06/16/2017	Minor updates for vote-by-mail campaign	1.0.4	Joni G. McNutt
07/21/17	Updated the About this document section to include references to individual product security specifications; added Ballot access controls and Ballot integrity sections to the Ballot management chapter; added information to the Power management and the Preventive maintenance sections; updated the Personnel section; added an introductory chapter; reorganized and restructured chapters for better flow.	1.0.5	Joni G. McNutt
09/25/2017	Added Physical security section, added Monitoring equipment section, updated Facilities section and Password management section, minor edits	1.0.6	Joni G. McNutt
01/19/2018	Vote-by-Mail campaign 2	1.0.7	Joni G. McNutt
04/13/2018	Minor edits	1.0.8	Joni G. McNutt
06/15/2018	Updated cover	1.0.9	Joni G. McNutt
08/03/2018	Added Decommissioning equipment section, updated the Election media section, added information that USB drives are encrypted, minor edits	1.0.10	Joni G. McNutt
08/15/2018	Updated cover	1.0.11	Joni G. McNutt

Table of contents

Preface 7

Chapter 1. Introduction 9

1.1 Security and encryption 9

Chapter 2. Equipment receipt 11

2.1 Acceptance testing 11

2.2 System configuration 11

Chapter 3. Managing voting equipment 12

3.1 Overview 12

3.2 Physical security 12

3.3 Malware 12

3.4 Ports 13

3.5 Election media 13

3.6 Power management 13

3.7 Supplies 13

3.8 Chain of custody 13

3.9 Decommissioning equipment 13

Chapter 4. Ballot management 14

4.1 Ballot access controls 14

4.2 Ballot integrity 14

4.3 Ballot content 14

4.4 Accessible ballots 15

4.5 Ballot testing 15

4.6 Printed ballots 15

4.7 Distribution 16

4.8 Voting 16

Chapter 5. Election preparation 17

5.1 Preventive maintenance 17

5.2 Loading the election onto voting devices 17

5.3 Delivery to the polls 17

5.4 Personnel 17

5.5 Facilities 18

Chapter 6. Logic and accuracy testing 19

6.1 Overview 19

6.2 Scope 19

6.3 Test pattern 19

6.4 Test criteria 20

Chapter 7. Personnel 21

Chapter 8. Password management 22

Chapter 9. Seals 23

9.1 Application 23

9.2 Logging 23

9.3 Election phases 23

9.4 Seal log 24

Chapter 10. Election Day 25

10.1 Equipment preparation 25

10.2 Polling place preparation 25

10.3 Report verification 25

10.4 Opening the polls 26

10.5 Voting 26

10.6 Monitoring equipment 27

10.7 Closing polls/Ending early voting day 27

10.8 Emergency evacuation 27

Chapter 11. Reporting/Aggregation 28

11.1 Reviewing reports 28

11.2 Results consolidation 28

Chapter 12. Reviewing and archiving 29

Chapter 13. Corrective maintenance 31

13.1 Overview 31

13.2 Documentation 31

13.3 Verification 31

13.4 Securing voting equipment/cast ballot information 31

Chapter 14. Transportation and storage 32

Preface

This section defines the purpose of this document. It contains the following subsections.

- About this document
- Scope of this document
- Intended audience
- Contact us

About this document

This document describes the procedural security protocol required for the ClearVote system, and complements the inherent security features that characterize the ClearVote products.

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

Scope of this document

This document includes the following sections:

- Introduction
- Equipment receipt
- Managing voting equipment
- Ballot management
- Election preparation
- Logic and accuracy testing
- Personnel
- Password management
- Seals
- Election Day
- Reporting/Aggregation
- Reviewing and archiving
- Corrective maintenance
- Transport and storage

Intended audience

This document is intended for election officials and election staff who are responsible for operations and maintenance before, during, and after an election. This document is also used by Clear Ballot personnel who support election officials and election staff.

Contact us

Clear Ballot Group welcomes your feedback on our documentation. Please send comments to Documentation@ClearBallot.com.

If you have questions about using your ClearVote product, contact your Clear Ballot representative.

Chapter 1. Introduction

The ClearVote system consists of four independent systems:

- **ClearDesign**—election management system
- **ClearAccess**—in-person accessible voting solution
- **ClearCast**—in-person precinct-scan voting solution
- **ClearCount**—central scan and tabulation, results consolidation and reporting

The diagram below shows the simple relationship between the independent systems. The ClearVote products exchange data in fully documented, zipped, plain text comma-separated values (CSV) files. These files are digitally signed for protection against tampering.

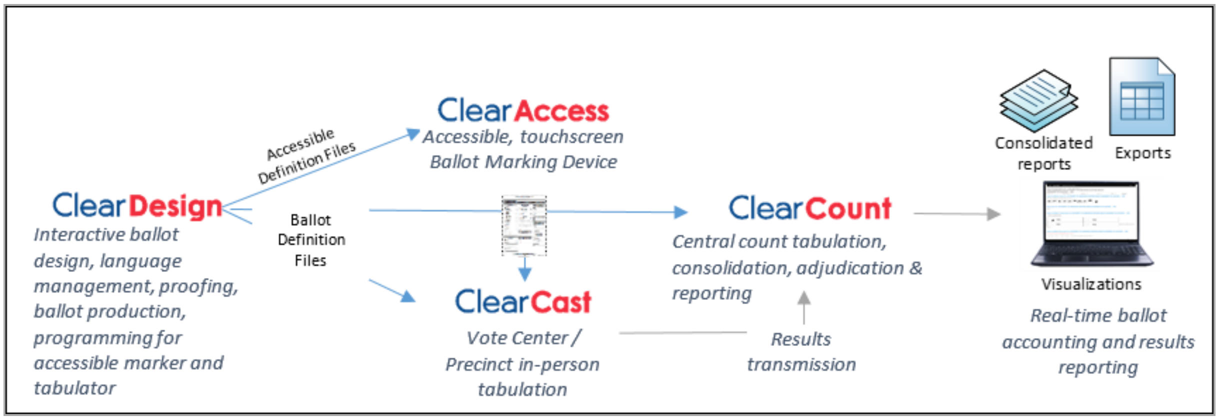

ClearDesign
Interactive ballot design, language management, proofing, ballot production, programming for accessible marker and tabulator
Accessible Definition Files
Ballot Definition Files
ClearAccess
Accessible, touchscreen Ballot Marking Device
ClearCast
Vote Center / Precinct in-person tabulation
ClearCount
Central count tabulation, consolidation, adjudication & reporting
Results transmission
Consolidated reports
Exports
Visualizations
Real-time ballot accounting and results reporting

Figure 1-1. Relationship between ClearVote systems

1.1 Security and encryption

Security is built in to the ClearVote system design and informs every technical decision. All networked components operate solely on closed, wired Ethernet connections. No component is ever connected to the Internet.

The ballot design system (ClearDesign) and the tabulating and reporting system (ClearCount) undergo a thorough hardening process to prevent unauthorized access. The accessible voter terminals (ClearAccess) and the precinct voting station (ClearCast) are also hardened with focus on the threat model associated with polling place deployment. The role-based security model establishes the minimum level of access (least privilege) that individual users are granted so that a jurisdiction can maintain control and accountability over system use.

When data is in motion in the ClearDesign and ClearCount systems, which operate on closed networks, it is encrypted to guard against interception, unauthorized viewing of the data traffic, and tampering with that data.

For enhanced security, the ClearVote system:

- Does not access the Internet.
- Does not use wireless or Bluetooth technology in its operations.
- Does not collect personally identifying information from voters.
- Enables the redacting of small vote totals in its ClearCount reports.

Chapter 2. Equipment receipt

2.1   Acceptance testing

An acceptance test should be performed for every piece of voting equipment received from Clear Ballot, whether it is new or repaired equipment. The acceptance test is a unique product-specific document for each ClearVote product. The acceptance test should be performed in accordance with the criteria provided in the official voting system documentation.

The results of the acceptance test should be recorded in the applicable product's acceptance test checklist. Any anomalies that arise during acceptance testing should be resolved according to the recommended resolution procedures, including the corrective maintenance procedures described in the voting system maintenance documentation. If any functional anomaly persists, voting equipment should be returned to Clear Ballot for resolution.

After the acceptance test has been successfully completed, the applicable voting equipment should be inventoried and stored according to storage conditions specified in the voting system documentation, and the completed acceptance test documentation archived.

2.2   System configuration

After it has successfully passed the acceptance test, the voting system must be configured using the procedures provided in the installation documentation for each product. System configuration may include equipment assembly, software configuration, system hardening, and network configuration.

The voting system may have been configured entirely or in part by Clear Ballot, in which case, only the outstanding configuration indicated for the voting system should be performed.

Software installation should typically be performed by Clear Ballot staff only. Any ClearVote software installed on voting equipment should be verified as being the correct certified software prior to installation. After software has been installed, an acceptance test should be performed to ensure that the software functions as expected.

Chapter 3. Managing voting equipment

3.1 Overview

Voting equipment should be used in conformance with the usage procedures and the environmental, transport and storage specifications provided in the associated product documentation, as well as local election management procedures and policy. State election officials and poll worker training staff are good sources of information pertaining to the polling place procedures required.

3.2 Physical security

Maintaining physical security of the ClearVote equipment is an important part of operations and maintenance. When the components of any system are not in use, they must be stored in a locked area under the custody and control of the jurisdiction. Access to this area must be controlled by the jurisdiction so the system cannot be accessed by unauthorized individuals, and so that any breaches in security can be recognized through the auditing functions of the system.

When in storage or in use, the ClearVote equipment must be kept within a controlled area where only individuals authorized by the jurisdiction to handle and process ballots, or to maintain the voting system, can come into direct contact with the ballots or components of the system. Each jurisdiction must also follow all jurisdictional and state rules for the handling and processing of ballots. This means that at least one security method is employed to provide deterrence and physical security:

- Receptionists or guards with a gate or other barrier to the scanning area
- Security cameras
- Electronic door-locking mechanisms such as ID cards or key fobs that record the identity of the device used to unlock the door
- A locking computer rack or other cabinet to contain components of the ClearVote system

The jurisdiction must record whenever any ClearVote equipment is brought out of storage. After setting up the system, examine the audit and system logs to determine if any unauthorized access occurred while the system was not officially in use.

If there is a break in the custody and control of the jurisdiction, the jurisdiction must reverify the integrity of the system and, if necessary, reinstall it.

3.3 Malware

The ClearVote voting system and associated election media must be maintained malware-free. This is achieved by keeping the voting system disconnected from the Internet, jurisdiction network, or any other public network; physically securing any rooms that contain election computers and voting machines; and practicing a culture of computing hygiene in all aspects of election operations.

3.4 Ports

Ports on ClearVote election devices are to be used exclusively for authorized election system components or malware-free election media. Unused ports must be secured by obstructing them with tamper-evident tape. The integrity of the tamper-evident tape must be verified on a regular basis before, during, and after an election.

At no point can any unauthorized hardware be connected to the ClearVote system. If an unauthorized connection does occur, system integrity must be reverified.

3.5 Election media

USB drives loaded with election information must be labeled with the appropriate voting location ID and machine ID (if multiple voting machines are used at the polls).

USB election media must be maintained free of any malware. Clear Ballot recommends the use of encrypted USB drives. See the *ClearVote Approved Parts List* for information about approved devices.

3.6 Power management

Election locations should be provisioned with appropriate uninterruptible power supply (UPS) devices, which are intended to guard against power loss during a power outage by providing a minimum of two hours of backup power for computers and other system devices. The specific UPS technology used at the polls or central-count location depends upon the ClearVote voting device deployed. See the *ClearVote Approved Parts List* for approved UPS devices.

3.7 Supplies

Only authorized supplies should be used with voting equipment, including ballot-marking instruments, thermal paper tapes, and ballot stock. All of the supplies designated for use with the ClearVote voting system are available for purchase from Clear Ballot.

3.8 Chain of custody

All voting equipment should be tracked using the appropriate chain-of-custody procedures and documentation.

3.9 Decommissioning equipment

When decommissioning voting equipment, jurisdictions must follow guidelines established by the US Election Assistance Commission (EAC) to ensure that equipment is disposed of in a secure manner. Contact your Clear Ballot representative if you need assistance in determining the necessary requirements for your equipment.

Chapter 4. Ballot management

4.1 Ballot access controls

The creation of BDFs and ADFs within ClearVote products is governed by strict security controls, including system hardening, network and database encryption, role-based user accounts with individual access levels, encrypted password-protected access, and FIPS 140-2 compliant cryptography. All user access and user actions are tracked in log files. Additionally, all activity regarding the BDFs and ADFs is logged.

All ClearVote log files are read-only. Their contents cannot be modified or deleted by any user. Log files are digitally signed to ensure that they have not been corrupted. If logging processes are stopped or are not available at startup, the user receives an alert and is not allowed to access the associated ClearVote software.

Jurisdictions are responsible for maintaining proper physical security for all computers and their networked systems. When the equipment is in use, a properly trained and trusted election official should be present in the room with the equipment at all times. When the equipment is not being used (for instance, between elections), the computers should be kept in a locked room. Entry to that room should be restricted, logged, and monitored.

4.2 Ballot integrity

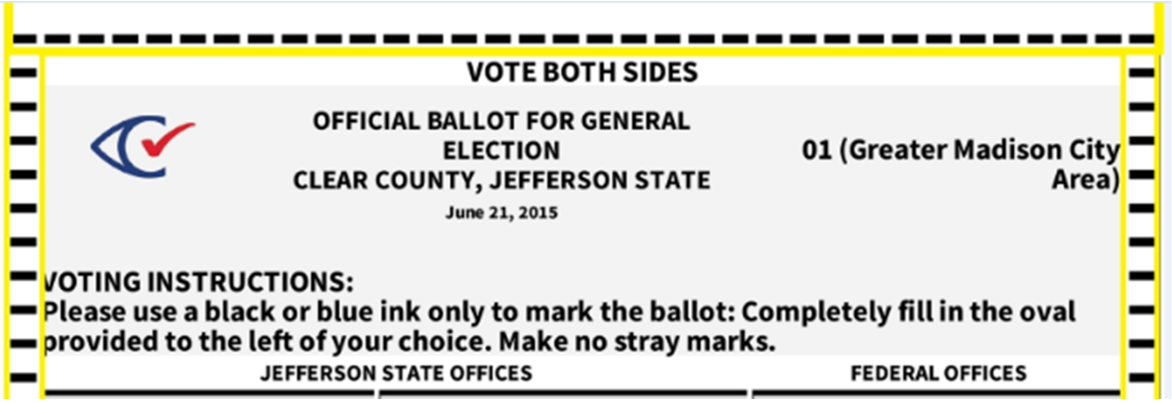
ClearVote BDFs and ADFs are encrypted via hash message authentication code (HMAC) technology to ensure integrity. The HMAC signature, which is a FIPS 140-2-compliant message digest of a password concatenated with the file contents, verifies that the file contents have not been tampered with. The HMAC signature requires a password when the BDF and ADF are loaded onto a ClearVote computer. Logging in to a ClearVote system automatically checks the HMAC of the BDF or ADF to guard against tampering or intentionally changing information.

4.3 Ballot content

All text and audio ballot content, in all applicable languages, should be arranged in the manner required by state and local law. Likewise, contests, as well as candidates and question responses, should be ordered as required, and subject to the locally mandated rotation requirements, where applicable. All text should be legible and clearly audible where applicable. The required special voting rules should be implemented so as to apply correctly and consistently to all applicable ballots.

The application of fonts and formatting should be performed in a strictly consistent manner, and be compliant with state and local law. All candidates and responses on the visual and audio ballots should be presented on the ballot in such a way that no individual selection would be perceived to be preferential.

The election architecture should ensure that every contest is assigned to the correct precincts and precinct splits. Clearly worded voting instructions should be positioned at the top of every printed ballot.



VOTE BOTH SIDES

OFFICIAL BALLOT FOR GENERAL ELECTION
CLEAR COUNTY, JEFFERSON STATE
June 21, 2015

01 (Greater Madison City Area)

VOTING INSTRUCTIONS:
Please use a black or blue ink only to mark the ballot: Completely fill in the oval provided to the left of your choice. Make no stray marks.

JEFFERSON STATE OFFICES

FEDERAL OFFICES

Figure 4-1. Voting instructions

4.4 Accessible ballots

Any language translations should be performed by accredited agencies only, and implemented into ballot content in a manner that is complete and correct.

Any election implemented with the ClearAccess accessible-voting system should allow every ballot type to be votable in a fully private and accessible manner. The equivalent of every printed ballot and all contest and candidate content must be available in an equivalent audio ballot in an election that supports accessible voting.

All audio content should be presented in a consistent and neutral voice.

4.5 Ballot testing

Every unique ballot style must be tested comprehensively using the logic and accuracy (L&A) testing procedures provided in the corresponding user documentation. These test procedures should ensure that every voting position on every ballot is marked, counted and tallied (as appropriate), and that no voting position that has not been selected is marked and counted. For more information on the pre-election ballot testing requirements, see "Logic and accuracy testing" on page 19.

The same printer should prepare ballots used for L&A testing as for official voting.

4.6 Printed ballots

Paper ballots should be printed on stock in conformance with the *ClearVote Ballot Stock and Printing Specification*. The layout, dimensions, cutting, and quantities of printed ballots should be inspected when received from the print shop.

Ballots received from the printer must be secured. Ballot quantities should be verified upon receipt from the printer, and any allocations to testing should be noted so that the quantities of all ballot styles can be accounted for at the end of the election.

4.7 Distribution

Absentee ballots should be prepared so that fold marks do not intersect voting ovals. Absentee ballots must be mailed in conformance with local deadlines.

Printed ballots should be delivered to the polls in sealed containers in precounted amounts. Seals on ballot containers received at polls should be verified and recorded prior to the polls opening.

Precinct workers should count out expected ballot quantities, and maintain a tally of ballots issued to voters.

Banded quantities of 50 or 100 ballots are generally better than ballots on tear-off pads, since tearing off the ballots may damage them or introduce unwanted debris in ballot scanners.

4.8 Voting

Ballots should be maintained secure at the polls during periods of voting. Ballots processed using ClearCount must be secured and logged.

ClearCast ballot boxes must be sealed and secured when they become full. Voted ClearAccess ballots must be housed in a secure receptacle, unless they are scanned immediately after voting and deposited automatically into a secure ballot box.

At the end of Election Day, voted ballots should be reconciled against initial ballot inventory. All blank, damaged and nonprocessed ballots must be returned to the warehouse in sealed containers. Ballot container seal numbers should be verified and recorded at the warehouse.

Chapter 5. Election preparation

This chapter describes the security considerations pertaining to the preparation of voting equipment for an election. Election preparation activities should be performed on election equipment prior to every election, and all preparation activities documented.

5.1 Preventive maintenance

Prior to every election, preventive maintenance must be performed on all ClearVote voting equipment using the maintenance procedures provided, including any prescribed cleaning and battery charging.

To provide continuous system operation in the event of a power outage, laptop computers must be charged overnight to ensure a minimum of two hours of battery-backup operation.

5.2 Loading the election onto voting devices

Election and ballot content, as well as voting instructions and audio, are loaded onto voting devices by means of the ClearVote ballot definition files (BDFs) and accessible definition files (ADFs). Loading these files is performed in tandem with the assignment of a counter group and voting location. BDFs and ADFs should be loaded onto ClearVote voting devices in a secure environment.

✓ Logging in to the ClearAccess, ClearCast, and ClearCount voting devices automatically checks the hash message authentication code (HMAC) of the BDF and ADF to guard against tampering or intentionally changing information.

After the loading and configuration of election information has been performed, review the application user interface to confirm this information. Election media compartments must subsequently be closed, locked, and sealed, and the seal numbers recorded.

5.3 Delivery to the polls

Prior to delivery to the voting locations, voting equipment and the associated supplies must be prepared in accordance with the information provided in the applicable product documentation.

Voting devices should be transported to the polls in sealed carrying cases.

5.4 Personnel

Election preparation must be performed only by authorized election officials, and their individual tasks documented and signed off.

5.5 Facilities

Election preparation activities involving voting equipment must be performed in secure facilities by authorized election officials.

The central-count scanning location must be secured. Unauthorized individuals must not be allowed into the facility. Individuals who are not part of the jurisdiction’s permanent staff must sign in and sign out at the entrance. The log of this activity must be maintained.

Chapter 6. Logic and accuracy testing

6.1 Overview

A public logic and accuracy test should be performed prior to every election as required by state and local law. A logic and accuracy test can also be performed following the election.

The same printer should be used to print test and official ballots.

Test election results reports should be printed and reviewed against manual tally sheets for every ballot style tested. For more information on report considerations, see "Reporting/Aggregation" on page 28.

All pre-election and logic and accuracy testing materials should be archived, including test ballots and test election results reports.

6.2 Scope

All ballot styles and voting devices in the election should be subjected to a comprehensive logic and accuracy test. The test should involve the full cycle of activity anticipated involving the ClearVote system, including:

- Voting (ClearAccess)
- Ballot printing (ClearAccess)
- Ballot casting (ClearCast)
- Ballot counting (ClearCast)
- Ballot counting (ClearCount)
- Results aggregation (ClearCast, ClearCount)
- Results reporting (ClearCast, ClearCount)

6.3 Test pattern

Every ballot style in an election should be tested using the following marking/voting scheme:

- One ballot with the first candidate/response selected in each contest
- One ballot with the second candidate/response selected in each contest
- And so on, until the last test ballot is marked/voted for the ballot style, with the last candidate/response selected in the contest with the highest number of candidates/responses

Alternatively, this test deck can also be composed as follows:

- One ballot with the first candidate/response selected in each contest
- Two ballots with the second candidate/response selected in each contest

- And so on, until a number of test ballots are marked/voted corresponding to the number of candidates/responses in the contest on the ballot with the highest number of candidates/responses, each of the ballots marked/voted in the last candidate/response position

6.4 Test criteria

The structure of the test may vary according to local requirements, but should be designed to reflect all:

- Ballot styles
- Precinct splits
- Parties (in a closed primary)
- Voting locations
- Languages
- Special voting rules
- Voting/Ballot-counting devices
  - Accessible voting devices (ClearAccess)
  - Precinct-count system (ClearCast)
  - Central-count system (ClearCount)

Chapter 7. Personnel

All election staffing roles must be clearly defined in terms of responsibilities (See the *ClearVote Personnel Deployment and Training Plan.*). Election personnel should be subjected to appropriate vetting (such as, performing background checks) and assigned unique system credentials (user name, password, access level). Knowledge of system access passwords must not be shared.

Every staff position should be provided the appropriate training with ClearVote products.

Physical access to voting equipment, supplies and facilities must be restricted to authorized personnel. Election personnel should only perform authorized duties. Reports, logs, and other materials should be reviewed at the end of the election to verify that staff members engaged within the scope authorized for their roles.

Chapter 8. Password management

Unique user passwords must be created for every election cycle, or at least annually. Clear Ballot recommends that passwords associated with user roles be composed as follows:

- A password must include eight characters or more (Clear Ballot recommends a minimum of 14)
- A password must not have consecutively repeating characters
- A password must not include any word found in a dictionary of any language
- A password must not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- A password must contain characters from three of the following four categories:
    - Latin uppercase characters (A through Z)
    - Latin lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example, !, $, #, %)

Knowledge of a user's password must be limited to the user, and not shared with anyone else, internal or external to the jurisdiction.

✓ Jurisdictions can devise their own password management protocols on the ClearVote client computers (ScanStations, election administration stations, DesignStations, ClearAccess touchscreen) via the Microsoft Windows Group Policy Editor (see the Microsoft Windows documentation for details).

Chapter 9. Seals

9.1 Application

Seals must be applied to all voting device compartment doors, as well as any exposed ports. Seals should be applied so that it is not possible to open a compartment door or access a port on the voting device without breaking the seal.

To ensure that any unauthorized access to the ballot box will be detected, seals should be applied to the ClearCast ballot box after it has been installed, as well as when the full box has been removed from the unit.

9.2 Logging

The following information should be recorded upon seal breakage/reapplication:

- Seal number
- Staff member
- Role
- Date and time
- Purpose

9.3 Election phases

Seal application/removal may occur in the following instances:

- Device configuration
- Device testing
- Installing election media
- Ballot testing
- Ballot box installation
- Polls opening
- Device installation
- Ballot box removal
- Equipment repair
- Polls closing
- Filing nonprocessed ballots
- Filing election media

9.4 Seal log

A seal log should be maintained for every voting device throughout the election cycle. At the end of an election, all equipment seal logs should be verified to ensure that no inappropriate access has taken place.

Chapter 10. Election Day

10.1 Equipment preparation

Precinct-voting devices must be configured at the polls according to authorized procedures.

Seals on precinct-voting device carrying cases must be verified and recorded prior to opening. Prior to precinct-voting device installation, poll workers need to verify that there are no ballots inside the ballot box. Poll workers also need to check the voting equipment display to ensure the correct firmware version is installed.

Configured voting device compartments and exposed ports must be sealed, and the seal numbers recorded.

After powering on and initial log in, precinct-voting devices should display the Polls Open menu.

10.2 Polling place preparation

Voting booths should be configured in a manner that ensures the voters optimal privacy, and should be equipped with marking instruments and voting instructions.

All ClearCast compartments should be closed, locked and sealed when not in use. When a compartment is opened, the seal number must be verified and breakage recorded according to local requirements.

Voting device keys should be kept in the possession of authorized poll workers at all times during official voting.

No unauthorized materials or people should be present at the voting locations.

10.3 Report verification

Prior to the start of official voting, all candidate and ballot counters on the Zero Totals reports must be confirmed as zero. Election officials reviewing the report should then sign the oath area at the bottom of the report (if present).

For the ClearCast voting station, the report should not be detached from the paper roll in the printer, and instead left attached to the Summary Totals Report when it is printed. The election media compartment should be left sealed until the encrypted USB drives have been removed after polls close.

The following information must be verified on the Zero and Election Totals reports in the context of logic and accuracy testing prior to the official voting:

- All contests applicable to the precincts supported at the voting location are present in the report
- No contests are present on the report that are not valid in the precincts supported at the voting location
- All contests are in the correct order on the report
- The correct candidates and responses are present in every contest
- All candidates and responses are in the correct nominal (nonrotated) order on the report
- All candidates/responses have the correct spellings
- All contest counts are zero

All test reports must be reviewed and archived.

10.4 Opening the polls

For in-person precinct voting, opening the polls for the ClearCast voting station consists of changing to the Polls Open mode after verifying the appropriate reports.

10.5 Voting

Voters should be provided with voting instructions and a secrecy sleeve prior to voting.

If paper ballots are one-sided, voters can be instructed to carry them to and feed them into the ClearCast voting station face down to aid in preserving privacy.

Poll workers should assist voters in resolving ballot return conditions without violating voting privacy. Where possible, poll workers should avoid observing marked ballots as they resolve ballot return conditions.

Poll workers should verify that:

- Each voting device monitor displays the Voting login or ballot insertion prompt at all times when not in use
- The scanner processes every cast ballot as expected
- Ballot counters increment on voting devices as expected

Any voting device that does not behave as expected in the course of voting/ballot casting should be serviced according to authorized procedures. Any serviced voting equipment must be properly tested prior to redeployment.

✓ No unauthorized access to voting devices must be permitted.

10.6 Monitoring equipment

At the polling location, each voting device must be monitored by election officials at all times, and the tamper-evident seals must be inspected regularly to ensure integrity.

10.7 Closing polls/Ending early voting day

Polls should be closed on voting devices at the designated election closing time. At the end of an early voting day, voting devices are placed in a Polls Closed status and then powered down, but the election is not "closed."

When Election Day has ended, the seal on the ClearCast election media compartment must be verified and the seal broken so that the two encrypted USB drives can be removed.

10.8 Emergency evacuation

In the event of an emergency evacuation at the polling location—and only then—the authorized poll worker should unlock and open the ClearCast voting station's election media compartment and remove both encrypted USB drives. The poll worker should keep the drives in his or her possession at all times until replaced in the voting station. Local law may also require poll workers to remove any blank and voted ballots in addition to the removable media.

Chapter 11. Reporting/Aggregation

11.1 Reviewing reports

For the ClearCast voting station, the Summary Totals report should be reviewed by poll workers, and all reviewing parties should sign the oath area at the bottom of the report (if present).

For every contest on the Summary Totals report, the contest times counted value should be reconciled with the candidate and response totals, write-ins, overvotes, undervotes and blank votes.

ClearCast reports should be sent to election central with the corresponding election media (encrypted USB drives) in sealed containers.

11.2 Results consolidation

After the ClearCast election data has been aggregated to the ClearCount system, the ClearCount election results reports should be printed, reviewed, and reconciled against the ClearCast Summary Totals reports.

All ClearCount election results reports should be reviewed prior to release outside of the tabulation area.

Chapter 12. Reviewing and archiving

At the end of an election, system and election audit logs from every voting device should be reviewed and archived in print or electronic form.

Audit logs should be reviewed for any of the following:

- Unexpected error conditions
- Security breaches
- Equipment malfunctions
- Actions involving unauthorized users

The following should be also be reviewed at the end of every election:

- ClearCast Election Summary Totals reports for each voting station
- ClearCount election results reports
- Seal logs
- Ballot reconciliation reports

Ensure that all documentation generated in the course of the election cycle is accounted for and archived. Any inconsistencies arising in the review of audit-related documentation must be investigated.

✓ Details regarding logs and log entries can be found in each ClearVote product's documentation.

The following documentation should be archived following every election:

- ClearCount Statement of Votes Cast report prior to beginning central-count scanning (the zero report)
- ClearCount database with aggregated results
- ClearCount Cast Vote Record
- ClearDesign ballot definition files
- ClearDesign accessible definition files
- ClearDesign election definition reports
- ClearCast Zero Totals reports
- ClearCast election results reports
- ClearAccess ballot reports
- Status reports
- Seal log sheets
- Project milestones

- Completed sign-off sheets
- Test ballot decks
- Logic and accuracy test decks, reports and tally sheets
- Manual tally sheets
- Audit and system reports

Some of these artifacts may correspond to components of the ClearVote system not in use by the local jurisdiction, and may mot be available. Furthermore, the specific artifacts archived in an election depends upon local requirements.

Chapter 13. Corrective maintenance

13.1 Overview

Repairs to voting equipment should be performed only by authorized personnel equipped with Clear Ballot-vetted training. Repairs should be performed using the approved repair procedures provided in the maintenance documentation for each voting device.

Any seals that are broken while performing repairs need to be recorded and replaced.

13.2 Documentation

Repairs should be documented with the following information:

- Technician
- Date and time
- Problem
- Resolution

13.3 Verification

After repairs have been completed:

- Targeted testing must be performed to verify that the repair has been successful.
- The appropriate seals must be reapplied and recorded.

If corrective maintenance has been performed on a ClearCast voting station during an election, the following information must be verified before resuming its use:

- Election name
- Voting location
- Number of ballots cast

13.4 Securing voting equipment/cast ballot information

Under no circumstances are the polls to be closed on a voting device with live election media before the official close of polls. Recuperation of the contents of election media to an alternate voting device/election media should be performed according to the designated procedure. Any voting devices or election media should be disposed of using the appropriate protocol, which may include its erasure and destruction by known repeatable methods.

Chapter 14. Transportation and storage

Voting systems should be transported using the designated transport cases. Any storage facility used to house voting equipment or ballots must be physically secured. Access to voting equipment should be managed using a chain-of-custody approach. Access to every voting device in storage should be tracked with the following information:

- Election official
- Role
- Date and time
- Purpose

Supplies should be inventoried with the corresponding voting device.

Storage of ClearVote voting equipment should occur according to the appropriate environmental conditions.