CONDITIONS OF USE FOR CLEAR BALLOT GROUP'S CLEARVOTE 2.3 VOTING SYSTEM

The Secretary of State promulgates the following conditions for use for Clear Ballot Group's ClearVote 2.3 voting system by political subdivisions of the state of Colorado, in accordance with section 1-5-608.5(3)(b), C.R.S. The Secretary of State reserves the right to revise, amend or supplement these conditions from time to time, in her discretion and as circumstances warrant.

Condition No.	Condition Statement
A. (ClearAccess-1)	Election Rule 20.5.2(e) prohibits counties from connecting any component of a voting system to the Internet. As a result, the ClearAccess tablets cannot automatically update the time that appears on the tablet displays. A variance between the time displayed on the ClearAccess tablet and the actual time does not affect or impair the accuracy, integrity or functionality of the in-person voting components of the voting system. Counties may, but are not required to, manually update the time on the ClearAccess tablets. When changing the time of ClearAccess tablets, the county must not change or alter any other tablet settings.
B. (ClearAccess-2)	The county must connect the components that lack onboard battery supplies of at least one accessible voting station to an uninterruptible power supply (UPS) with battery backup of at least 2 hours. These components include the ClearAccess tablet and the accompanying printer.
C. (ClearAccess-3)	The county must seal the ClearAccess tablet according to the procedures in Appendix A.
D. (ClearAccess-4)	If the county secures a polling location in which the ClearAccess components are deployed against unauthorized entry or access before and after the polling location's regular hours of operation, the county may leave the ClearAccess components in a connected state during times when the polling location is closed, from the date on which the county opens the polling location for business until the day after Election Day. The county may also store the ClearAccess components in a connected state during the storage time if all other storage requirements required by election rule are maintained. For purposes of this Condition D (ClearAccess-4), the "ClearAccess voting station components" include the ClearAccess tablet contained within its enclosure, the EZ Access keypad if applicable, and the accompanying ClearAccess ballot printer. The county must seal the connected USB port and the empty Ethernet port to the printer according to the procedures in Appendix A.
E. (ClearAccess-5)	Modifications for ClearAccess stations that use the Dell Optiplex 5250 All-In-One computer must be performed per the *Equipment Modification for EAC Test Compliance: ClearAccess™* documentation.
F. (ClearAccess-6)	Modifications for ClearAccess stations that use the Elo E-Series (15" screen) computer must be performed per the *ClearAccess 2.1 Hardware Compliance Addendum* documentation.

G. (ClearAccess-7) Modifications for ClearAccess stations that use the Elo X-Series (20" screen) computer must be performed per the applicable portions of the *ClearAccess 1.5 Hardware Compliance Addendum* documentation.

H. (ClearAccess-8) Deleted

I. (WebSCORE-1) When processing voters in WebSCORE, election judges must select "IN-PERSON DRE" as the ballot type for all in-person voters that use the ClearAccess ballot marking devices.

J. (Server-1) Reinstallation of the trusted build is not required in the event that a hard drive used in a RAID configuration has to be replaced, as long as the replacement hard drive is installed per Clear Ballot Group's or the computer manufacturer's documentation.

K. (Passwords-1) Passwords must be updated according to the schedule in Appendix C.

L. (ClearDesign-1) The county must include the text "Ballot Style" and the Ballot Style keyword in the headers for both ClearAccess printed ballots and paper ballots. The county must verify the presence of the text "Ballot Style" and the Ballot Style keyword in the headers of ClearAccess printed ballots and the artwork for paper ballots before the county prints ballots on demand, or finalizes its ballot printing order with a third-party print vendor.

M. (ClearCount-1) In order to facilitate the risk-limiting audit, the county must segregate and secure scanned ballots in the same order in which they were scanned and by batch number.

N. (ClearCount-2) The county must calibrate each ballot scanner before conducting the logic and accuracy test required by Rule 11.3.2, by using Clear Ballot Group's calibration sheet and instructions in Chapter 10 of the *ClearCount Election Preparation and Installation Guide*.

O. (ClearCount-3) For elections with multi-card ballots, the voting system increases by one the number of ballots cast each time the first ballot card is scanned. If a voter fails or omits to return the first card of multi-card ballot, the county must insert a blank first card as a placeholder before the ballot cards comprising the ballot are scanned. The county may, but is not required to, similarly insert before scanning blank placeholder cards for any missing second or subsequent card of a multi-card ballot. The county may add a unique mark or stamp to an area that cannot be tabulated of all blank placeholder cards, in order to quickly identify them and expedite their digital adjudication. The county must adopt processes that

preserve voter anonymity in determining whether blank placeholder cards will be inserted before scanning multi-card ballots.

P. (ADJ-1) The clerk and recorder must appoint an adjudication team consisting of two election judges to work at each adjudication workstation. The county clerk must appoint adjudication team members so that each adjudication team is a validly constituted resolution board in accordance with Election Rule 18.3.2(c). Each adjudication team must resolve markings on ballots sorted for adjudication by the voting system in accordance with the most recent version of the Secretary of State's Voter Intent Guide. Since the individual members comprising an adjudication team may change from time to time during the election cycle, and in order to maintain an audit record of the individual election judges who resolved each adjudicated ballot in the election, the county must require the members of each adjudication team to record the dates and times of their work.

Q. (RSD-1) When inserting removable media into any workstation or component of the voting system (other than ClearAccess), the county must manually scan the media with Windows Defender:

1. Click the **Start** button in the lower left corner, scroll down the list to **Windows System** and select **Windows Defender** from the dropdown menu.
2. Select **Custom** from the scan options on the main screen and click **Scan now**. Select the drive with your inserted removable media by checking the box and click **OK**.

R. (RSD-2) In accordance with Election Rule 20.6.2., and unless explicitly permitted by the exceptions listed in paragraphs 1-5 of this Condition, the county may not insert a removable storage device into any workstation or component of the voting system unless (a) the device is obtained from a trusted source and has never been used previously, b) the county first reformats a previously used device on an air-gapped computer or reformatting device that has not been connected to the internet since its acquisition by the county, or (c) the device is hardened against malware and approved for use by the Secretary of State, and the county uses the built-in controls to erase or reformat the device after it has been used on an internet-connected computer.

A previously used removable storage device containing data may be inserted into a voting system workstation or component only under the following circumstances:

1. The device contains only election definition data downloaded from SCORE in compliance with Election Rule 20.6.2(b);
2. The device contains only election and ballot style data files downloaded from the EMS workstation in compliance with Election Rule 20.6.2(c) that is used to prepare a BMD for testing or use in an election;

3. The device contains only database and project files programmed by a third-party programming service provider in compliance with Election Rules 20.6.2(d) and Condition S (RPS-1) below;
4. The device contains only anti-virus and malware definitions and files downloaded from the Secretary of State's SFTP site from a SCORE workstation, if the removable device was never used or is reformatted in accordance with this Condition before its insertion into the county workstation that access the SFTP site; or
5. The device contains data that is authorized in writing by the Secretary of State.

S. (RPS-1) The county must not copy to, install on or import into any workstation or other component of the voting system, a database, project or other file programmed or created by a third-party programming service provider, unless the third party provides the county with a signed affirmation certifying compliance with the requirements of Election Rule 20.8, in a form approved by the Secretary of State.

T. (CVR-1) Deleted

U. (ENR-1) The county must convert the ClearVote election night reporting (ENR) export file to a format compatible with Scytl's ENR software by using the utility certified with the ClearVote voting system.

V. (Security-1) The county must seal the case of each computer with tamper evident seals sufficient to prevent the case of the computer from being opened without removing the seals. The county must record the serial number of every seal on the appropriate chain-of-custody log. Two individuals must verify, and indicate by signing and dating the log, that the seal serial numbers match the logged serial numbers. For examples, please refer to Appendix B.

W. (Security-2) A county must secure the hard drive slots on the front of the server with the front bezel included with the server. The bezel must be locked, and tamper evident seals must be placed over the bezel on each end. The key for the bezel must be stored in a secure location. The county must record the serial number of every seal on an appropriate chain-of-custody log. Two election officials must verify, and indicate by signing and dating the log, that the seal serial numbers match the logged serial numbers. For an example, please refer to Appendix B.

Appendix A –ClearAccess Seal Locations

A. Procedures for sealing the Okidata B432dn printer:

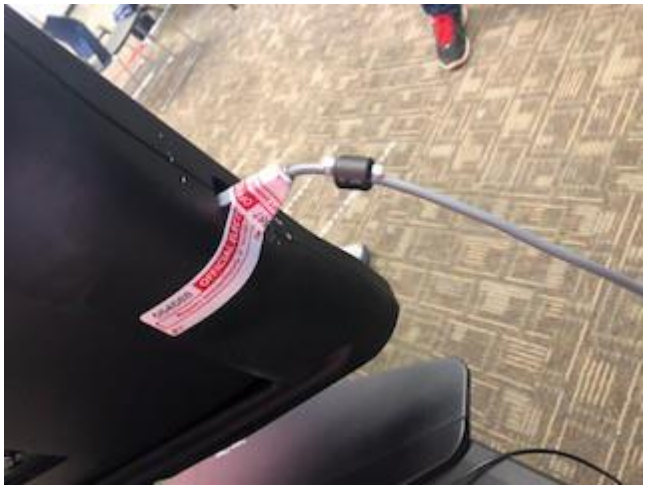
1. Use two seals. After plugging the USB cable into printer, wrap one seal around the cable as close to the printer as possible creating a tail pointing down that is able to stick to the printer.

2. Stick the tail over the Ethernet port.

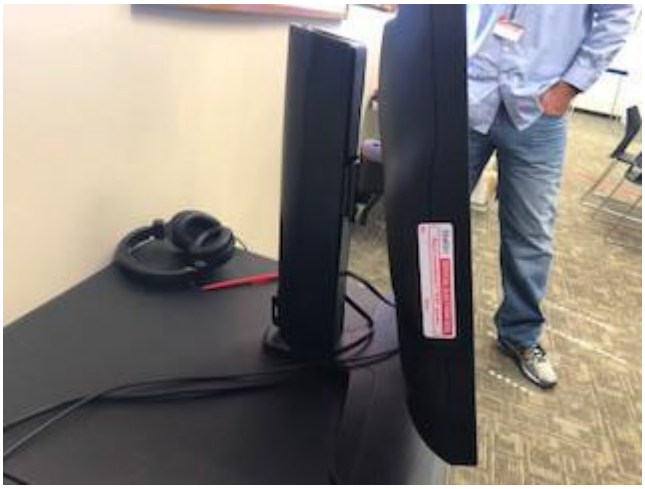
3. Place the second seal over the tail of the first seal and the Ethernet port and log the second seal number.

B. Procedures for sealing the ClearAccess all-in-one:

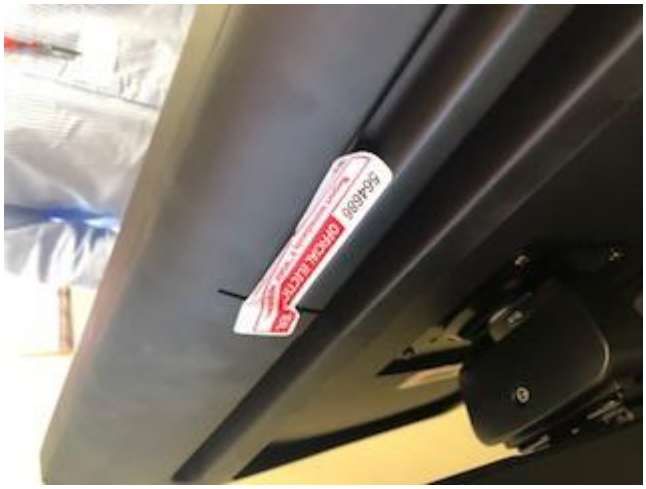
1. If the ClearAccess all-in-one is connected to the ATI, in a similar manner to the Okidata B432dn printer, plug in the ATI USB cable to the all-in-one. Apply a seal to both the all-in-one and USB cable (with as much surface area covered by the seal on both the cord and all-in-one as possible, and making sure the seal number is on the all-in-one). Wrap another seal around the end of the USB cable, covering the first seal (making sure the number on the second seal is visible). Record both seal numbers.



2. If the ClearAccess all-in-one is not connected to the ATI, apply a seal over the opening in bottom of the bezel that covers the opening entirely. Record the seal number.

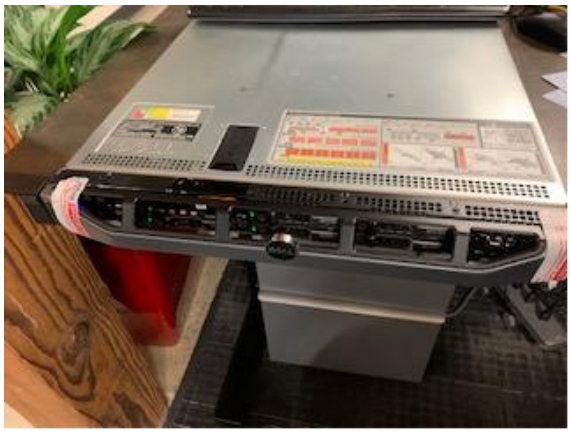


3. Apply a seal to one of the screw grooves on the back of the bezel, making sure the screw is covered by the seal. Record the seal number.

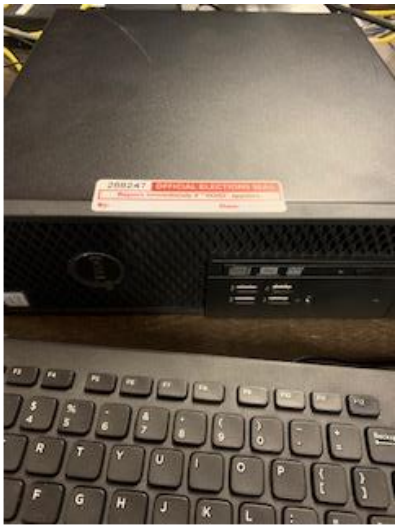


Appendix B Computer Seal Locations

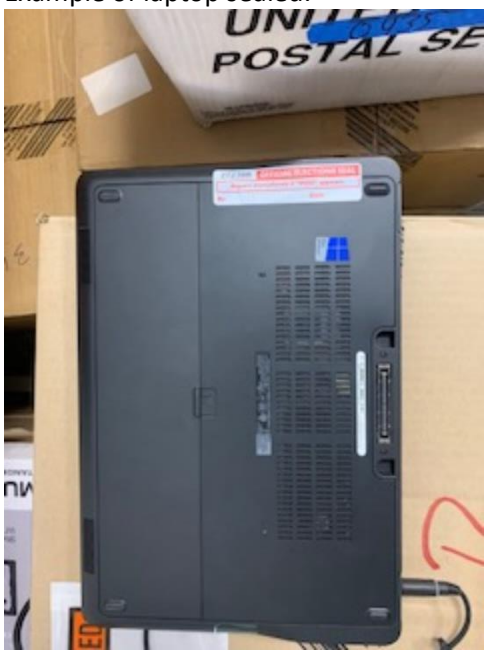
Server Seal example, with bezel:



Example of tower computer sealed:



Example of laptop sealed:



Appendix C – Password Schedule

Password	Must Change:
UNIX	Only at trusted build
MySQL	Only at trusted build
Windows admin accounts	Once per year
Windows user (staff) accounts	Once per year
Windows user (election judge) accounts	For each election
ClearDesign Admin	Once per year
ClearDesign User	For each election
ClearCount Admin	Once per year
ClearCount User	For each election
ClearCount Adjudication Station	For each election
ClearCount Scan Station	For each election
ClearAccess Windows Admin	Once per year
ClearAccess Windows ClearAccess (User)	Once per year
ClearAccess Admin PIN	Once per year
ClearAccess Maintenance PIN	Once per year
ClearAccess Poll Worker PIN	For each election
ClearAccess Voter PIN	For each election