## Conditions of Use for Dominion Voting Systems' Democracy Suite® 5.17 Voting System

The Secretary of State promulgates the following Conditions of Use for Dominion Voting System's Democracy Suite® 5.17 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. (ICX-1) | Condition Deleted. |
| B. (ICX-2) | For each VSPC, the county must connect at least one accessible voting station to an uninterruptible power supply (UPS) with battery backup of at least 2 hours. These components include the ICX and the accompanying ICX printer. |
| C. (ICX-3) | Except as alternatively provided in Condition D (ICX-4), the county must disconnect, re-seal with tamper-evident seals, and document in the ICX chain-of-custody log, the USB connector of the printer cable and the USB plug of the USB cable or the RJ-45 plug of the cable that is used to connect the Audio Tactile Interface (ATI) accessibility device, when each ICX is not deployed for an election or is in storage. |
| D. (ICX-4) | The county must seal the ICX devices at the locations specified in Appendix A to these Conditions. If the county secures a polling location in which the ICX components are deployed against unauthorized entry or access before and after the polling location's regular hours of operation, the county may leave the ICX 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 ICX 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 (ICX-4), the "ICX voting station components" include the ICX Classic, the ATI, if applicable, and the accompanying ICX ballot printer. |
| E. ~~(~~ICX-5) | Condition Deleted. |
| F. (ICX-6) | Condition Deleted |
| G. (ICX-7) | Condition Deleted. |

H. (ICX-8) If the county deploys ICVA laptops at VSPCs to program ICX voter activation cards, the supervisor judge in each VSPC must assign at least one election judge to collect ICX voter activation cards immediately after a voter concludes a voting session on an ICX device. Without compromising the voter's privacy in any way, the responsible election judge should monitor and collect the voter card from the voter immediately after the voting session terminates and the voter deposits his or her ICX ballot into the ballot box. The county must direct election judges to instruct voters to keep the voter activation card in the ICX until the ballot has printed completely. The county must also instruct election judges that if an error occurs because a card was removed before printing was completed, the judge must clear the error message and inform the voter to ensure their choices are reflected on the printed ballot correctly.

I. (ICX-9) Each county must label each pollworker card and voter card with a unique identifying number. Before and after the VSPC opens and closes each day, the supervisor judge must verify that all pollworker and voter cards issued to the VSPC are present and accounted for. If at any time the supervisor judge cannot account for all voter activation cards originally issued to the VSPC, the supervisor judge or a member of the county's elections staff must immediately report the issue to the Secretary of State by emailing an incident report to voting.systems@ColoradoSOS.gov.

J. (ICX-10) Before storing ICXs, authorized county staff must verify the remaining battery charge is between 50-80%, turn off the devices, and ensure they are not connected to an external power source. The county should monitor the remaining battery charge during extended storage and recharge them when the battery charge falls to 20% or less.

K. (ICX-11) In addition to Condition J (ICX-10), when powering off the ICX Avalue (Classic) device for storage, the county must use the "Prepare for storage" option in the technical administration menu to preserve the battery life.

L. (ICVA-1) If deployed for use at a polling location, the county must securely store each ICVA laptop in a locked storage area before and after the polling location's hours of operation.

M. (ICVA-2) Before storing ICVA laptops, authorized county staff must verify the remaining battery charge is between 50-80%, turn off the devices, and ensure they are not connected to an external power source. The county should monitor the remaining battery charge during extended storage and recharge them when the battery charge falls to 20% or less.

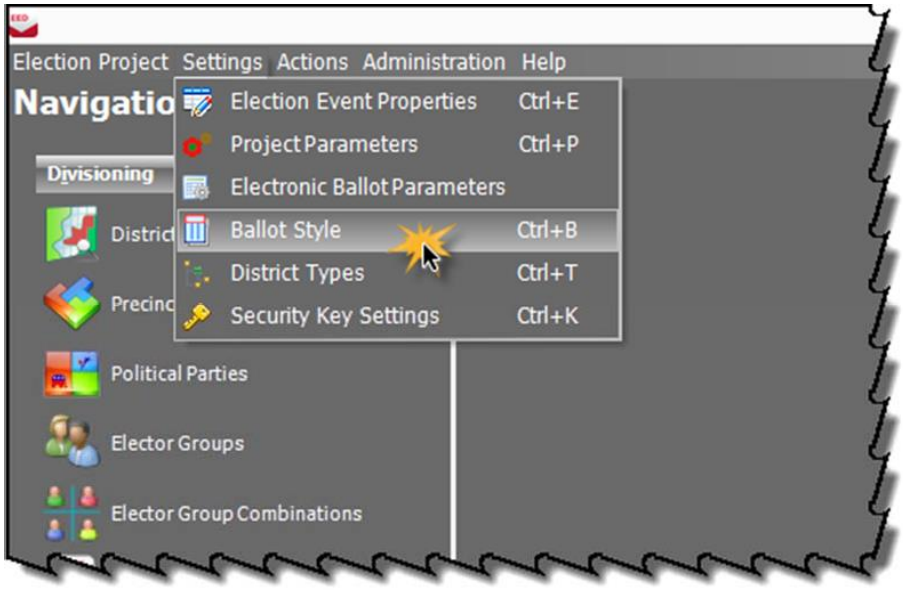
N. (WebSCORE-1) When processing voters in WebSCORE, election judges must select "IN-PERSON BMD" as the ballot type for all in-person voters that use the ICX ballot marking devices.

O. (EMS 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 Dominion's or the computer manufacturer's documentation and approved by the voting systems team.

P. (Passwords-1) Passwords must be changed based on the passwords schedule in Appendix C.

Q. (EED-1) New projects in Election Eventer Designer (EED) default to having the Dominion copyright notice printed on the ballots. Counties must disable this feature after each project is initially created by following the steps below:

1. Open the Project.
2. Select **Settings** >> **Ballot Style**.




3. Uncheck the checkbox next to **Draw Copyright Tag.** Also, verify the checkbox next to **Use Black Polling Box is** selected**.**

4. Click **Apply**, then click **OK**.

R. (EED-2) All ballot PDFs default to the CMYK color format suitable for printing on the Runbeck BOD printer and Dominion MBP. Counties adding their own instructional images to the ballots must ensure that the images are in the proper CMYK format.

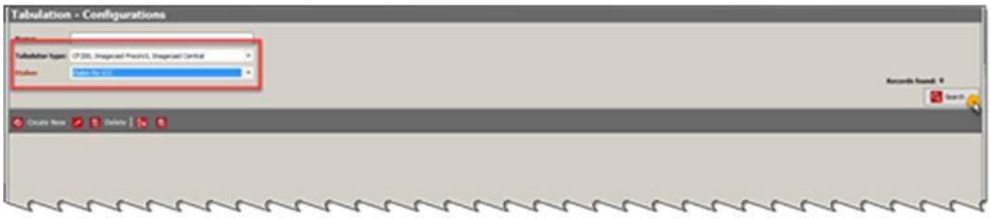
S. (EED-3) Counties may not use the QR code ballots. All counties must configure their systems for ICX ballot marking devices to print uniform ballots during ballot programming.

Counties must set the scanning parameter low scanning threshold to no higher than 12% and the high scanning threshold to no lower than 35%.

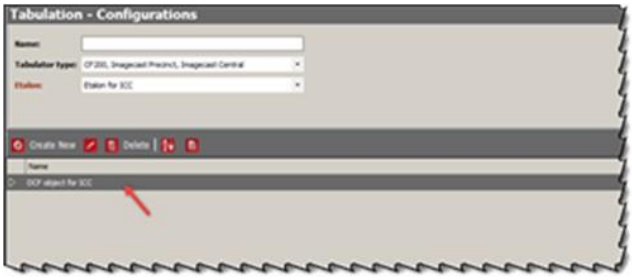
T. (EED-4) The county must set the write-in threshold to the same minimum settings as those in Condition S (EED-3). In addition, in accordance with Rule 18.5.3(b), the county must program the election to detect and sort for adjudication any ballot where writing appears in the write-in area, whether or not the corresponding target area is also marked. This must be done before generating election files in the Device Configuration File (DCF) that is created/edited in EED, as follows:

1. Log into the election project in EED.
2. Expand the **Tabulation** section on the left **Navigation** menu.
3. Select **Configurations**.

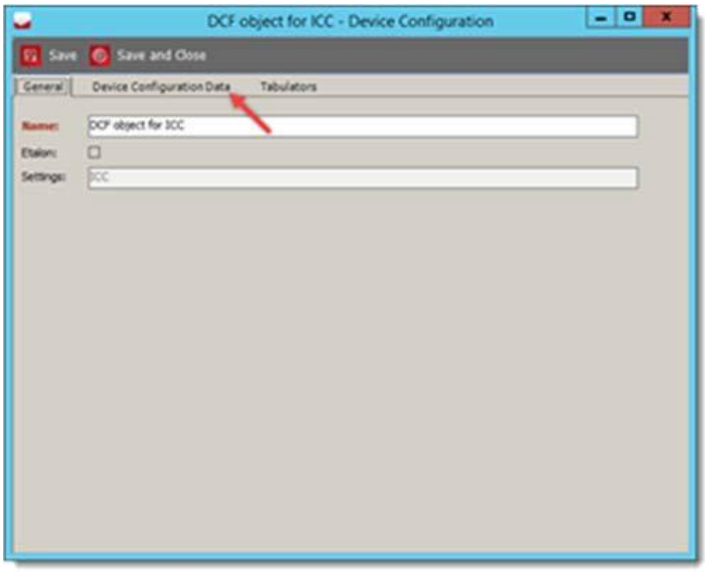
4. Select the following search parameters.
   a. Tabulator Type = CF200, ImageCast Precinct, ImageCast Central
   b. Etalon = Etalon for ICC



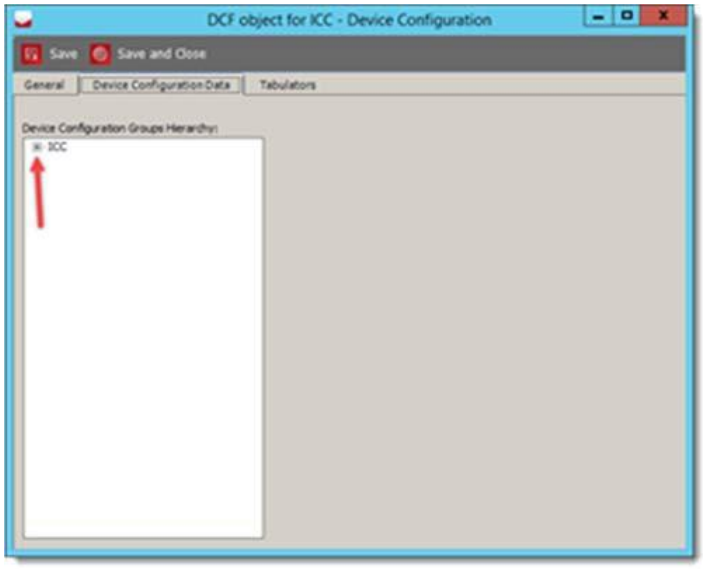

5. Click on the **Search** button.
6. Double click on the item called **DCF object for ICC**.



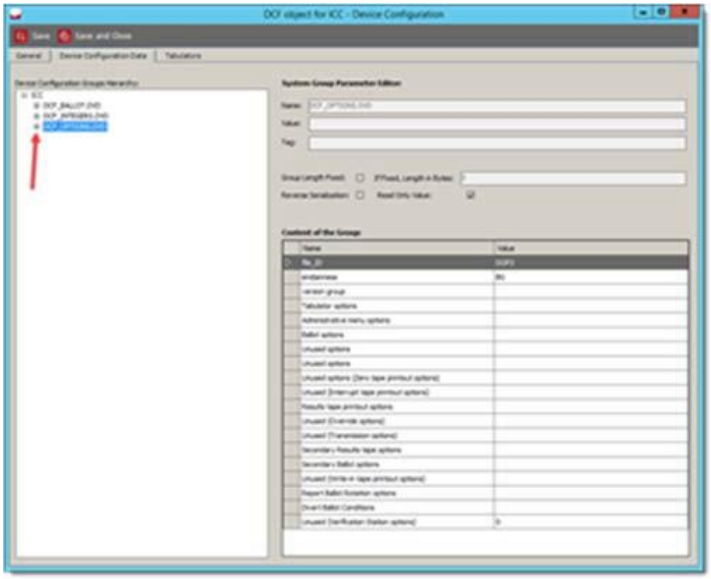
7. Select the **Device Configuration Data** tab.



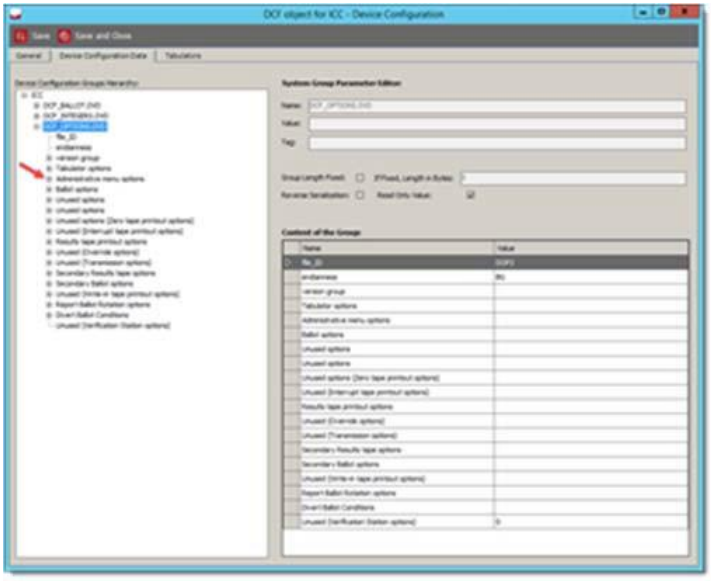

8. Expand the **ICC** menu to view all the submenus, by selecting the **+** sign next to **ICC**.



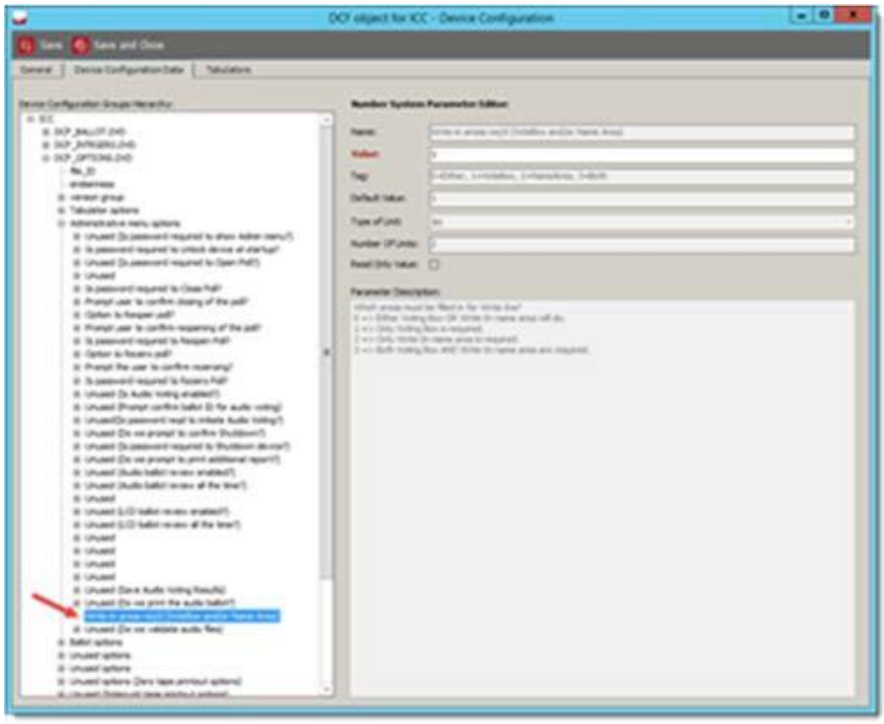
9. Expand the **DCF_OPTIONS.DVD** submenu.



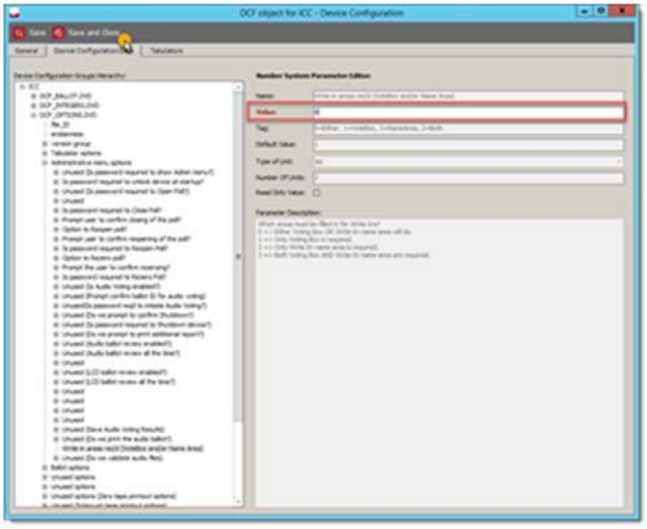
10. Expand the **Administrative menu options** submenu.



11. Select the **Write-in areas req'd (voteBox and/or Name Area** option.



12. Set the **Value** field to 0. This allows for write-in detection to look at either the voting box (target area) or the Write-in Name area.



13. Click **Save and Close**.

U. (EED-5) Condition Deleted.

V. (EED-6) The county must include the text "Ballot Type" and the Ballot Type keyword in the headers for both ICX and paper ballots. The county must verify the presence of the text "Ballot Type" and the Ballot Type keyword in the headers of ICX 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.

W. (EED-7) A county that uses election staff to build the election database and layout ballots in the voting system (rather than engaging Dominion to provide those services) may use the project template created by Dominion for the specific type of election in question and the version of the voting system being used by the county and authorized for use in Colorado by the Secretary of State.

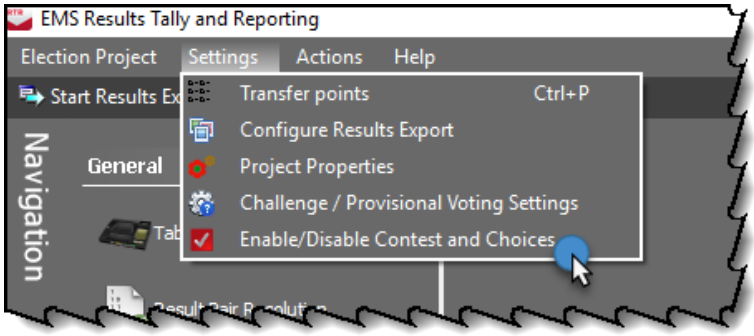
X. (EED-8) Condition Deleted.

Y. (EED-9) When defining the election in EED, the county must begin their ImageCast Central tabulator numbers with number 101. All tabulator numbers must be consecutive (i.e., 101, 102, 103, etc.).

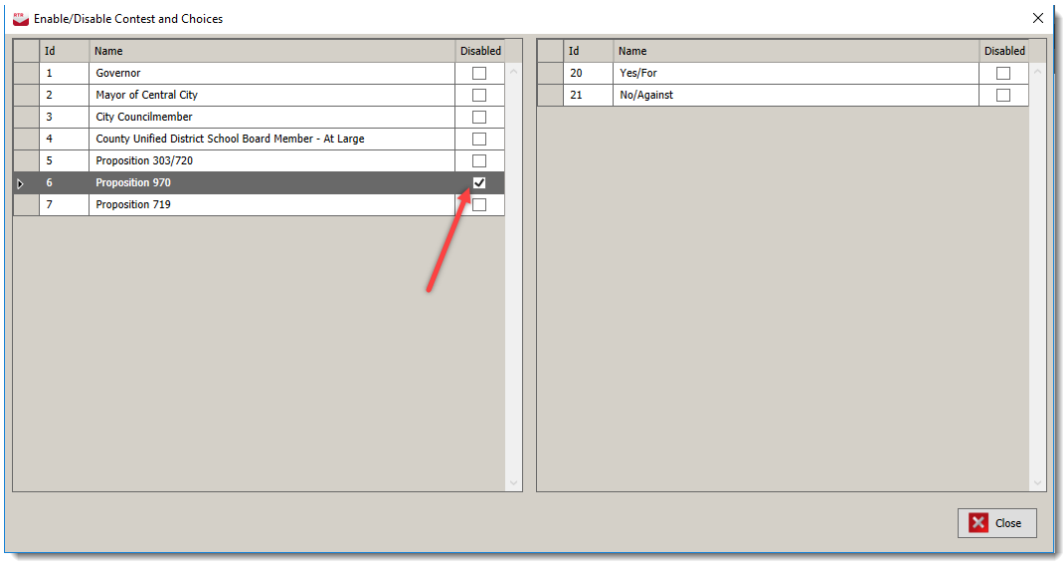
Z. (RTR-1) If a) the designated election official withdraws a ballot contest, b) the only candidate in a ballot contest withdraws, or c) a ballot includes a contest for which there are no candidates for the office in question, the county must disable the ballot contest in RTR before generating results reports. The county must notify the Voting Systems team so that the contest can be disabled in ENR.

To disable a ballot contest in RTR:

1. Open the Election Project in RTR.
2. From the Top menu, select **Settings**.
3. From the **Setting**s drop down menu, select **Enable / Disable Contest and Choices**.



4. Locate the contest you wish to disable in the Contest List. Select the checkbox in the **Disabled** column next to the **Contest Name**.




AA. (RTR-2)

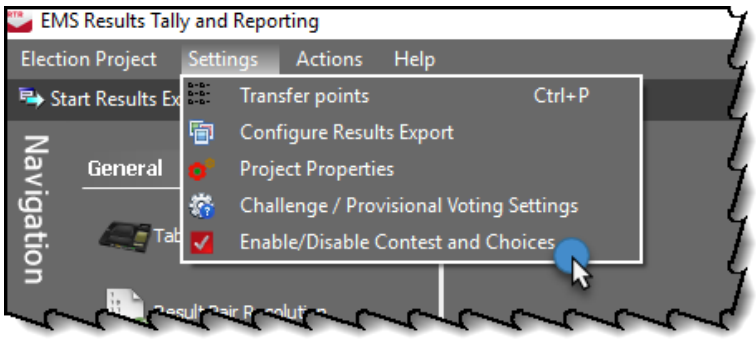
If a candidate in a contested ballot contest withdraws, the county must disable the candidate in RTR before any summary report is released or any ENR zero report is generated. The county must notify the Voting Systems team so that the candidate can be disabled in ENR.

To disable a withdrawn candidate in a contested contest in RTR:

1. Open your Election Project in RTR.

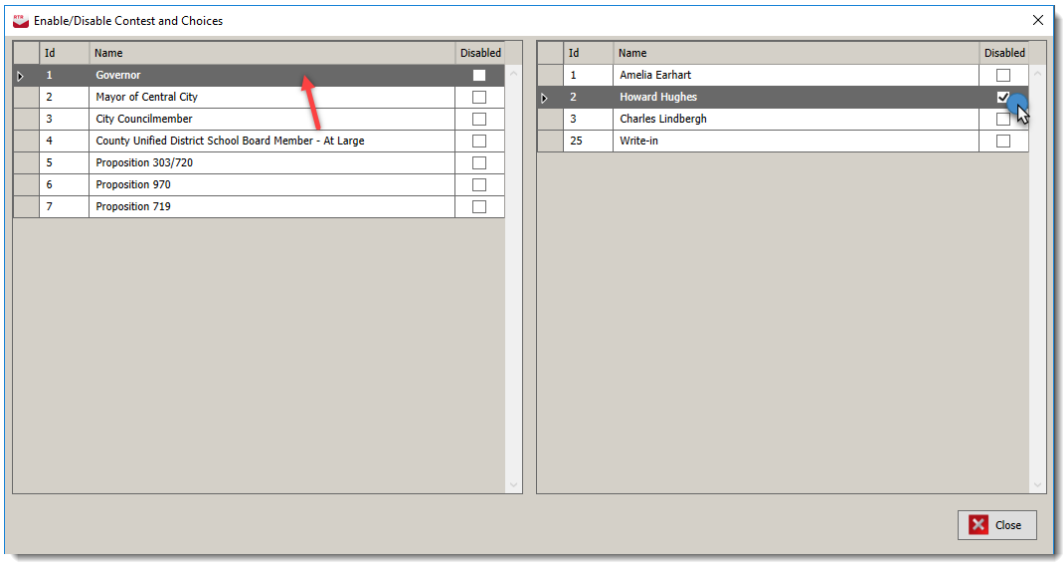
2. From the Top Menu, select **Settings.**

3. From the **Settings** drop down menu, select **Enable / Disable Contest and Choices.**




4. Select the contest the candidate is withdrawing from. This will populate the candidate list at the right.

5. Select the checkbox in the **Disabled** column next to the candidate name.




6. Select Close from the lower right-hand corner of the window.

To un-disable (or enable) a withdrawn candidate before resuming ballot scanning and adjudication, follow the above steps but **un**-check the **Disabled** box at the bottom of the window in Step 4, and choose **Save and Close.**

BB. (EDT-1) Before importing the SCORE election definition export file into Election Data Translator (EDT), the county must (a) convert the SCORE election definition export file format from .xls to .xlsx, and then (b) update the .xlsx file to the current EDT file format, according to the instructions provided by Dominion.

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

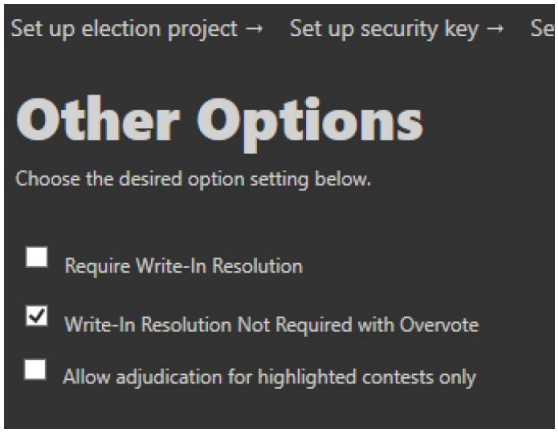
DD. (ICC-2) Counties must not utilize any color drop-out, including red drop-out, in the scanner settings in the ICC application.

EE. (ICC-3) The county must calibrate each ballot scanner before conducting the logic and accuracy test required by Rule 11.3.2, by using Dominion's calibration sheet and instructions.

FF. (ICC-4) 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.

GG. (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.

HH. (ADJ-2) The County must not select "Allow adjudication for highlighted contests only" in adjudication unless the adjudication is occurring during a recount.




II. (RSD–1) Unless a county is using the onboard functionality of the state provided Aegis USB drive to format the device, when inserting removable media into any workstation or component of the voting system (other than an ICX), the county must manually scan the media with Microsoft Defender.

1. Click the **Start** button in the lower left corner, scroll down the list to

**Windows System** and select **Microsoft 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**.

JJ. (RSD-2) In accordance with Election Rule 20.5.3(c), 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 any of the following circumstances:

1. The device contains only election definition data downloaded from SCORE in compliance with Election Rule20.5.3(c)(2);
2. The device contains only election and ballot style data files downloaded from the EMS workstation in compliance with Election Rule 20.5.3(c)(3) 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 20.5.3(c)(4)and Condition KK (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 accesses the SFTP site; or
5. The device contains data that is authorized in writing by the Secretary of State.

KK. (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 20.8.1, in a form approved by the Secretary of State.

LL. (CVR-1) The county must delete the Counting Group column, if it exists, from the cast vote record (CVR) export file before hashing and uploading the CVR file to the Secretary of State in accordance with Rule 25.2.2.

MM. (DUP-1) If a paper ballot includes an instruction advising voters to correct mistaken or erroneous markings by crossing out the incorrect choice and marking the target area next to the correct choice, election judges must visually inspect before scanning, at a minimum, all ballot styles containing a multi-vote (vote-for-two or -more) ballot contest. If the corrected marking creates an overvote condition that will result in the corresponding ballot image being queued to the voting system's adjudication application for resolution by a bipartisan team of election judges, the ballot may be scanned. If the corrected marking does not create an overvote condition, a bipartisan team of election judges must physically duplicate the ballot to reflect the voter's intent and then scan the duplicate ballot, in accordance with Election Rule 18.4 and the Secretary of State's Voter Intent Guide.

NN. (Security-1) The county must seal the case of each workstation (including ICC-all in ones and ICVA laptops) 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 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 examples, please refer to Appendix B.

OO. (Security-2) A county with a standard server 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. If a county does not have a bezel to secure access to the hard drive slots, the county must place a seal over each set of hard drive slots on the server, including slots which do not have any hard drives. 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 examples, please refer to Appendix B.

## Appendix A ICX Seal Locations

Unless the Secretary of State gives written approval in advance of alternate seal locations and chain-of-custody procedures, the County Clerk and Recorder (or his or her designee) must affix tamper-evident seals at the following locations of the ICX in-person voting components:

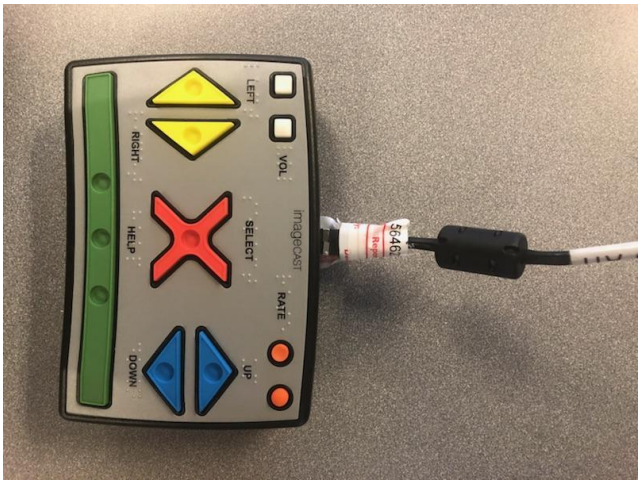
Upper Door Seal:

Lower Door Seal:

## ATI Seals:

1. Use two seals. After plugging the cable from the ICX into the ATI, attach the seal over the back of the ATI and wrap around the cable.


2. With the second seal, wrap around the end of the fist seal that is attached to the cable, make sure that the seal number is visible on both seals.

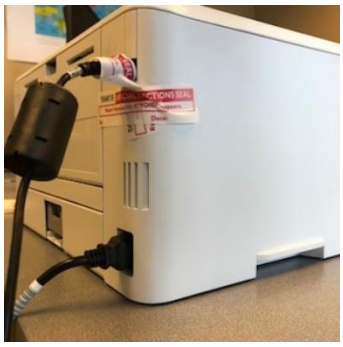



## Printer Seals:

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.



## Storage Seals:

When not in use any loose cables should have a seal covering the end of the cable:

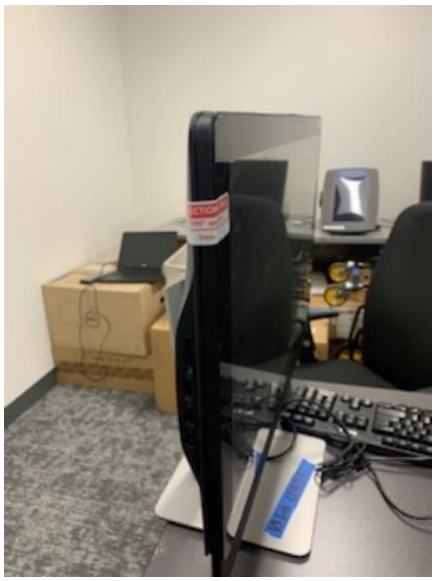
## Appendix B Computer Seal Locations

Standard Server Seal example, without bezel:

Standard Server Seal example, with bezel:

Example of tower computer sealed:

Example of All-In-One (ICC) sealed:



Example of laptop sealed:

## Appendix C Password Schedule

| Password | Change |
|---|---|
| Tech Card PIN | Once per year |
| Pollworker Card PIN | Once per Election |
| iButton | Once per Election |
| Admin/Tech Advisor Project User Account | Once per Election |
| RTR User Account | Once per Election |
| Windows Admin Account | Once per Year |
| Windows User Account | Once per Election |