Rule 20. County Security Procedures

20.1 Security plan

20.1.1 The county clerk must submit their county security plan on the form prescribed by the Secretary of State in accordance with section 1-5-616(5), C.R.S., no less than 60 days before an election. A county clerk may amend their county security plan within 60 days of an election as a result of an unforeseen circumstance. The county clerk must document the changes and file the revisions with the Secretary of State within five days of the change.

20.1.2 In the security plan, the county clerk must provide the following information:

(a) Sample copies of all security forms, schedules, logs, and checklists they will use in the upcoming election;

(b) Detailed plans regarding the transportation of equipment and ballots to remote voting sites and back to the central elections office or storage facility;

(c) The details of the security training it will provide, including the time, location, and number of election officials receiving the training, in accordance with Rule 20.3;

(d) The name, title, and date a background check was conducted for each employee for whom the county clerk is required to perform a background check under Rule 20.2.3;

(e) All voting system acceptable use policy agreements signed by county staff which had not previously been provided in a security plan that calendar year;

(f) A description of the environment in which voting system components will be kept in accordance with Rule 20.5.5; and

(g) Any other information required in the published security plan.

20.2 Background checks

20.2.1 Background checks generally

(a) A person may not access the systems, information, or access controls outlined in this Rule 20.2 until a background check of that person has been performed and passed.

(b) A background check that is required by this Rule 20.2 must be run at least once per calendar year, prior to the first election of the year. In a year in which a presidential primary will be held, the background check may be performed in December in the year prior to the presidential primary.

(c) Unless otherwise noted, a background check required by this Rule must be requested from the Colorado Bureau of Investigation.

(d) A background check may only be considered to have passed if the check finds that the person has not been convicted of:

(1) An election offense; or

(2) An offense with an element of fraud.

20.2.2 The county clerk must perform a background check for all election judges. In accordance

with section 1-6-101, C.R.S., an individual convicted of election fraud, any other election offense, or fraud may not serve as an election judge.

20.2.3 The county clerk must perform a background check in accordance with this Rule for each permanent or temporary staff member with access to:

(a) The statewide voter registration database;

(b) Elector's confidential or personally identifiable information;

(c) Voter registration applications or other list maintenance activities;

(d) A component of the county's voting system while at a location or during transport;

(e) Removable media that contains an election project backup; or

(f) A code, lock, combination, password, or encryption key for:

(1) Voting equipment;

(2) Ballot storage area;

(3) Counting room;

(4) Location of adjudication workstations; or

(5) Location of tabulation workstation.

20.2.4 A voting system provider must arrange for a background check, sufficient to determine if the individual has ever been convicted of an election offense or an offense with an element of fraud for each employee or contractor who conducts work on any component of a county's voting system. The provider must affirm that the check was conducted in writing to the Secretary of State prior to the employee conducting any work.

20.2.5 The Department of State must perform a criminal background check for each staff member who conducts work on any component of a county's voting system, and the staff member must pass the background check prior to conducting that work.

20.3 Security training

20.3.1 The county clerk must conduct security training for all field technicians who work on voting system components, contractors who work on voting system components or in a voter service and polling center, and election officials, if those technicians, contractors, or election officials are contracted with or otherwise work under the direction of the county clerk.

20.3.2 The security training required by this Rule must include the following components:

(a) Proper application and verification of seals and chain-of-custody logs;

(b) How to detect tampering with voting equipment, memory cards, or election data on the part of anyone coming in contact with voting equipment, including election officials, vendor personnel, or voters;

(c) Ensuring privacy in voting booths;

(d) Chain-of-custody requirements for voting equipment, activation cards, and other election materials;

(e) Ballot security;

(f) Voter anonymity; and

(g) Recognition and reporting of security incidents.

20.4 Physical security

20.4.1 Requirements for codes, locks, and combinations

(a) The county clerk must maintain restricted access to secure ballot areas and secure equipment areas as defined by Rules 1.1.48 and 1.1.49, by use of a code, lock, or other combination. This may include the use of a key card access system which also logs entry into the secure area.

(b) The county clerk may only give the code, lock, or combination required by this Rule to employees who have passed a background check in accordance with Rule 20.2.

(c) The county clerk must change the code, lock, or combination required by this Rule at least once per calendar year prior to the first election of the year.

20.4.2 Surveillance of secure areas

(a) The county clerk must make video security surveillance recordings of secure equipment areas, as defined by Rule 1.1.49, in accordance with the requirements of section 1-7-513.5, C.R.S.

(b) The county clerk of a county with 50,000 or more registered voters must also make video security surveillance recordings of secure ballot areas, as defined by Rule 1.1.48, if those areas do not contain any components of a voting system, beginning at least 35 days before election day and continuing uninterrupted through at least 30 days after election day. If a recount or contest occurs, the recording must continue through the conclusion of all related activity.

(c) The video security surveillance recording system must:

(1) Ensure that records are not written over when the system is full;

(2) Provide a method to transfer the video records to a different recording device or to replace the recording media; and

(3) If replaceable media is used, provide a process that ensures that the media is replaced often enough to prevent periods when recording is not available.

(d) The county clerk must adequately light the areas subject to video surveillance in this Rule to ensure visibility for video recording.

(e) Planned maintenance of video surveillance

(1) If necessity requires it, a county clerk may temporarily cease video surveillance of voting system components or other areas for planned maintenance of the video surveillance system, but only for so long as the interruption of surveillance is required.

(2) Before the planned outage, the county clerk must notify and submit detailed plans to the Secretary of State which describe security measures the clerk will take to ensure the security of the voting system components or areas

during the planned outage.

(3) After review of the plans, the Secretary of State may require a county clerk to take additional or different actions to ensure the security of voting system components or areas during the planned outage.

20.4.3 Access logs to secure areas

(a) The county clerk must maintain a log of each person who enters a location which contains components of a voting system in accordance with the requirements of section 1-7-513.5, C.R.S.

(b) The county clerk must otherwise maintain a log of each person who enters a secure ballot area, as defined by Rule 1.1.48, if that area does not contain any components of a voting system. This does not include members of the public who access areas of a county clerk's office that are regularly available to the public outside of an election.

(c) A log required under this Rule must contain the:

(1) Name of the person accessing the area; and

(2) Year, month, day, hour, minute, and whether the time is a.m. or p.m. that the area was accessed.

(d) If a log is generated by use of a key card or similar door access system, that system must be capable of producing a printed paper log that meets the requirements of this Rule.

20.4.4 Restrictions on physical access

(a) General restrictions

(1) No person may be present in a secure ballot area, as defined by Rule 1.1.48, or secure equipment area, as defined by Rule 1.1.49, unless:

(A) They are employees authorized to have a code, lock, or combination to the area under Rule 20.4.1;

(B) They are supervised by employees authorized to access that area; or

(C) They are emergency personnel responding to an emergency situation. In the event emergency personnel access this area without supervision, the county clerk must inform the Department of State as soon as they have knowledge of the event, and it is reasonably safe to do so.

(2) In extreme circumstances, the county clerk may request, and the Secretary of State may grant, an exemption from the requirements of this Rule.

(b) Individuals delivering ballots between separate rooms must wear distinguishing identification.

20.4.5 Remedies

(a) In the event that a county clerk discovers that a violation of Rule 20.4 has occurred, they must file an incident report required by Rule 20.12.2(a).

(b) The Department of State may take any action under Rule 20.12.2(b) to remedy a violation of Rule 20.4.

20.5 Security of voting system

20.5.1 Chain-of-custody requirements

(a) County clerks must continuously comply with the seal requirements of the most recent conditions of use issued by the Secretary of State for the county's voting system. County clerks may not allow any unattended voting system component to remain unsealed at any point after trusted build has been installed on a component.

(b) The county clerk must maintain and document uninterrupted chain-of-custody for each voting system component from the installation of trusted build to the present, throughout the county's ownership or leasing of the device.

(c) To maintain uninterrupted chain-of-custody for each voting system component the county clerk must:

(1) Record the serial number of every seal required by the conditions of use on the appropriate chain-of-custody log; and

(2) When removing or replacing seals, use two election officials to verify, and indicate by signing and dating the log, that the seal serial numbers match the logged serial numbers. The election officials should be of different party affiliations whenever possible.

20.5.2 Accessing the voting system

(a) Acceptable use policy agreement

(1) All election officials, who as part of their duties may be required to access any component of the voting system, must sign the voting system acceptable use policy agreement provided by the Secretary of State every year prior to using the system.

(2) The county clerk must submit copies of all newly signed acceptable use policy agreements signed by election staff with the county's security plan.

(b) Except for voters using a voting system component to vote during an election, a county clerk may not allow any person to access any component, including the hard drive(s) or copies of any part of the hard drive(s) for any component, of a county's voting system unless:

(1) That person has passed the background check required by this or any other Rule or law; and

(2) That person is performing a task permitted by the county clerk or the Secretary of State that is permitted by statute or rule, and is:

(A) An employee of the county clerk;

(B) Appointed as an election judge by the county clerk in accordance with Article 6 of Title 1, C.R.S.;

(C) An employee of the voting system provider for the county's voting system; or

(D) An employee or designee of the Secretary of State.

(c) Accounts and passwords

(1) The county clerk must change all passwords associated with a voting system according to the schedule required by the most recent conditions of use for that voting system.

(2) The county clerk may use the administrative user account for the election management system only to create individual user accounts for each election project.

(3) The county clerk must create individual user accounts that are associated and identified with each individual authorized user of the operating system of the voting system, election management system, or election project. If a particular election activity involves two election judges interacting with a voting system on the same activity, then the county may assign a single user account to both election judges for that activity. Both election judges must still comply with the log requirements of Rule 20.5.2(d).

(4) The county clerk must restrict access to each individual user account with a unique password known only to each individual user. Authorized users must access the operating system of the voting system, election management system, and election project using their individual user account and unique password.

(5) The county clerk may grant administrative privileges to no more than four individual user accounts per election unless the county clerk has requested and been authorized by the Secretary of State to grant more. The county clerk must identify the employees with administrative privileges in the security plan filed with the Secretary of State.

(6) The county clerk may only grant administrative privileges for the operating system of the voting system to the county clerk, employees of the county and the county clerk, and any person appointed by the Secretary of State to assist in the administration of an election, subject to the restrictions of Rule 20.5.2(c)(9). The county clerk may only grant administrative privileges to the election management system or the election project to the county clerk, employees of the county clerk's office, and any person appointed by the Secretary of State to assist in the administration of an election, subject to the restrictions of Rule 20.5.2(c)(9).

(7) Authorized users with administrative privileges of the operating system, election management system, or election project may not share their accounts or passwords with anyone.

(8) The county clerk must disable all accounts to access the operating system for individuals who are no longer employed by the county or are no longer employed in a role that requires access to the voting system.

(9) Any individual who is prohibited from having physical contact with any voting equipment under section 1-5-607(1), C.R.S., may not grant themselves or be granted with an account or password for the operating system of the voting system, the election management system, or an election project.

(10) The voting system provider may not have administrative or user access to the county's election management system.

(11) The civil servants at the Department of State will securely and confidentially maintain all BIOS passwords for voting system components.

(d) In addition to the audit logs generated by the election management system, the county clerk must maintain contemporaneous manual access logs that accurately record the date, start and end time, user's name, and purpose for each beginning and end of access of a component or application of the voting system.

20.5.3 Connecting to the voting system

(a) System settings

(1) If any component of the voting system is equipped with Wi-Fi capability or a wireless device, the county clerk must ensure that the wireless capability or device is disabled before use in an election.

(2) The county clerk may not alter, or grant permission to anyone else to alter, except during the trusted build process, the pre-boot settings for any voting system component, including altering the boot path.

(b) External network connection forbidden

(1) The county clerk must use the voting system only on a closed network or in a standalone fashion.

(2) The county clerk may not connect or allow a connection of any voting system component to the internet.

(3) The county clerk may not connect any component of the voting system to another device by modem.

(c) Removable storage device

(1) The county clerk must reformat all removable storage devices immediately before connecting them to any component of the voting system, except as provided in Rule 20.5.3(c)(2)-(5), or in the conditions of use.

(2) The county clerk may connect to the election management system, without first reformatting, a removable storage device containing only election definition data files downloaded from SCORE if:

(A) The county clerk reformats the removable storage device immediately before inserting it into the SCORE workstation and downloading the election definition data files; and

(B) Before and while downloading the SCORE election definition data, the county clerk installs and operates the advanced network monitoring and threat detection applications provided or approved by the Secretary of State.

(3) The county clerk may insert, without first reformatting, a removable storage device into a BMD, if:

(A) The removable storage device contains only election and ballot style data files necessary to program the BMD for testing or use in an election;

(B) The county clerk downloaded the election and ballot style data files directly from the election management system workstation;

(C) The county clerk did not expose the removable storage device to the internet or insert it into an internet-connected device after downloading the election and ballot style data files from the election management system; and

(D) The county clerk reformatted the removable storage device immediately before inserting it into the election management system and downloading the election and ballot style data files.

(4) The county clerk may insert a removable storage device into the election management system without first reformatting it, if the removable storage device contains only election database or project files remotely programmed by the voting system provider, in accordance with Rule 20.8.1.

(5) The county clerk may insert a removable storage device into the election management system without first reformatting it, if the removable storage device contains only election database backup files created by the county clerk and:

(A) The county clerk submits an attachment with their security plan stating security procedures for the removable storage device that addresses storage of the device when not in use; and

(B) The plan in the attachment is approved by the Secretary of State.

(d) The county clerk may not install any software on any component of the voting system unless directed to, or approved by, the Department of State.

(e) Activation cards

(1) The county clerk must assign and securely affix a permanent unique identifier to each removable card or activation card. The county clerk may use the manufacturer assigned serial number for this purpose.

(2) The county clerk must handle activation cards in a secure manner at all times. The county clerk must transfer and store any card or activation card in a secure container with at least one seal. Upon delivery and receipt, election judges or county personnel must verify, and indicate by signing and dating the chain-of custody log, that all seal numbers match those listed in the log.

(3) The county clerk must maintain a written or electronic log to record activation card seals and track seals for each voting unit.

(4) The county clerk must maintain a complete inventory of activation cards, including which VSPC they are assigned to during an election. Before and after a VSPC opens and closes each day, the supervisor judge must verify that all cards issued to the VSPC are present. If at any time the supervisor judge cannot account for all activation cards issued to the VSPC, the county clerk must immediately submit an incident report to the Secretary of State under Rule 11.7.

(f) No person may manually connect anything to a voting system component that enables a wireless connection. This includes, but is not limited to, external or additional network interface cards, other wireless antennas, or USB mice or keyboards that utilize wireless communication.

20.5.4 Transporting voting system

(a) The county clerk must submit detailed plans to the Secretary of State before the transportation of voting system components from a county election facility to another location, including a voter service and polling center. After review of the plans, the Secretary of State may require a county clerk to take additional or different actions to ensure the security of voting system components during transit.

(b) During or after transportation, if there is any evidence of possible tampering with a seal, or if the seal numbers do not match those listed in the chain-of-custody log, the county clerk must be immediately notified and must file an incident report required by Rule 20.12.2(a).

(c) Voting system components are not required to be under video security surveillance while in transit. In the plan required by Rule 20.5.4(a), the county clerk must describe how they will maintain bipartisan chain-of-custody while the components are not under video surveillance.

(d) Personnel requirements for transportation

(1) Transportation by county personnel

(A) County personnel must at all times display identification provided by the county.

(B) Two employee signatures and the date are required at the departure location verifying that the equipment is sealed to detect tampering. Upon delivery of equipment, at least two election officials must verify, and indicate by signing and dating the chain-of-custody log, that all seals are intact and that the seal numbers match the logged seal numbers.

(2) Transportation by election judges. Two election judges of different party affiliations that are receiving or transporting equipment must inspect all voting devices and verify the specific seal numbers by signature and date on the chain-of-custody log for the device.

(3) Transportation by contract

(A) If a county clerk contracts for the delivery of equipment, each individual delivering equipment must successfully pass a criminal background check as required by Rule 20.2.1.

(B) Two election officials must verify the specific seal numbers by device, sign, and date the chain-of-custody log upon release of the equipment to the individuals delivering the equipment. If the equipment is delivered by a truck capable of being locked by using a padlock or other similar device from the outside, the county clerk must provide a lock for the truck to be used during delivery. The county clerk must maintain the key or combination to the lock to be used to open the truck upon delivery. Upon delivery of equipment, at least two election officials must verify, and indicate by signing and dating the chain-of-custody log, that all seals are intact and that

the seal numbers match the logged seal numbers.

(C) A county clerk must require a contractor to deliver equipment on the day the equipment is picked up from the county clerk.

20.5.5 Storage of voting system

(a) The county clerk must keep all components of a voting system in a temperature-controlled storage environment that:

(1) Maintains a minimum temperature of 50 degrees Fahrenheit and a maximum temperature of 90 degrees Fahrenheit; and

(2) Is dry with storage at least four inches above the floor.

20.5.6 Retention of voting equipment

(a) If a county retains voting system components after the termination of a license agreement with a vendor, the county clerk must reformat any of those voting system components as directed by the Secretary of State, and the county clerk may not:

(1) Use the equipment for any other purpose until the components have been reformatted; or

(2) Transfer the components to any other department within the county or any party outside the county until the computers have been reformatted.

(b) All security standards in this Rule 20 are still applicable to voting system equipment until the components have been reformatted.

(c) Before the components are reformatted, the county clerk must preserve all election records required to be preserved by Rule 20 found on the voting system.

(d) These requirements also apply to any equipment that a county clerk no longer uses as voting system equipment but retains while a license agreement with a vendor is in force.

20.5.7 Use of voting equipment by other jurisdictions

(a) A county clerk may not transfer any voting system components to any municipality, special district, or another local jurisdiction, except to another county clerk and recorder.

(b) If a county clerk transfers any voting system components to another county clerk within the state, the receiving county clerk must follow all security procedures required by statute or these rules throughout the time they have custody of the components.

(c) A county clerk who is transferring voting system components to another county clerk must notify the Secretary of State of the transfer by filling out an acquisition/disposition form and transmitting it to the Secretary of State. The form must be filled out at both the time of the transfer to and transfer from the county clerk receiving the components.

20.5.8 Remedies

(a) Generally

(1) In the event that a county clerk discovers that a violation of Rule 20.5 has occurred, they must file an incident report required by Rule 20.12.2(a).

(2) The Department of State may take any action under Rule 20.12.2(b) to remedy a violation of Rule 20.5.

(b) In the event that an election official knows, or reasonably should know, that the county's voting system was accessed by any individual not permitted access by these Rules or is made aware that the system has been tampered with, they must immediately notify the Secretary of State.

20.6 Trusted build procedures at a county

20.6.1 When trusted build required

(a) In the event that the Secretary of State determines a trusted build is required in a county, including due to a new certification, modification, or other security issue, the county clerk and voting system provider must coordinate with the Secretary of State to install trusted build on a schedule determined by the Secretary of State's office.

(b) At the time that the Secretary of State determines a trusted build is required, the Secretary of State will provide the reason to the county clerk for the required trusted build.

20.6.2 Attendance at trusted build

(a) The only individuals who may be present at a trusted build in a county include:

(1) Secretary of State staff, designees of the Secretary of State, or other individuals approved by the Secretary of State;

(2) Voting system vendor staff for the voting system for which trusted build is being installed. At least one individual listed in Rule 20.6.2(a)(2) must be present during the trusted build, unless exempted by the Department of State; and

(3) The county clerk, employees of the county clerk, or the designated election official of the county, as long as those individuals are authorized to access the voting system under Rule 20.5.2(b) have signed the voting system acceptable use policy agreement, and subject to the restrictions of Rule 20.4.4(c). At least one individual listed in this Rule 20.6.2(a)(3) must be present during the trusted build.

(b) The county clerk and voting system vendor must provide the name and position of individuals who will attend the trusted build in a county at the time of scheduling the trusted build with the Secretary of State.

(c) Background check

(1) Any individual present at the trusted build must have had a background check conducted in accordance with Rule 20.2.

(2) The county clerk and voting system vendor must provide proof that a background check was conducted and passed on individuals who will be present to the Secretary of State at the time of scheduling the trusted build with the Secretary of State's office.

(d) The county clerk and voting system vendor may only allow the number of people designated by the Secretary of State for that county to attend the trusted build.

(e) If, due to an unforeseen circumstance, the county clerk or voting system vendor must send an individual not previously identified to the trusted build, the county clerk or vendor must immediately contact the Secretary of State and provide the information otherwise required by this Rule to the Secretary of State for the substitute individual.

20.6.3 Security at trusted build

(a) The county clerk must ensure that the location where the trusted build will be conducted does not allow for individuals who are not permitted to attend to be present or to otherwise disrupt the trusted build process.

(b) Video surveillance recording

(1) The county clerk must ensure that the trusted build is conducted under video surveillance as defined by Rule 1.1.61.

(2) The county clerk must identify the video surveillance equipment that will be used to comply with this Rule to those attending the trusted build.

(3) Video surveillance of the trusted build must be maintained as an election record under section 1-7-802, C.R.S.

(4) No one may surreptitiously record the trusted build by video or audio.

20.6.4 Completion of trusted build

(a) The county clerk must seal all voting system components in accordance with the most recent conditions of use issued by the Secretary of State for the county's voting system immediately upon conclusion of the trusted build unless the county clerk proceeds to and completes acceptance testing on the same day that trusted build is completed.

(b) In the event that the conditions of Rule 20.6.4(a) are met, the county clerk must seal all voting system components in accordance with the most recent conditions of use issued by the Secretary of State for the county's voting system upon conclusion of the acceptance testing.

(c) The county clerk must submit a copy of the signed trusted build affidavit to the Secretary of State following the completion of acceptance testing.

20.6.5 In the event that a trusted build cannot be scheduled or completed due to a county clerk's violation of these Rules or in the event that a county clerk is found to have violated these Rules following a trusted build, the Secretary of State may take any of the actions listed in Rule 20.12.2(b).

20.7 Security of ballots

20.7.1 Unvoted ballots

(a) The county clerk must secure unvoted paper ballots during pre-election storage, transportation, and at polling locations.

(1) Except when election judges are actively issuing ballots the ballot containers must be sealed.

(2) The county clerk must maintain chain-of-custody logs for all ballot containers.

(b) Unvoted paper ballots must be transported to polling locations in sealed containers. The county clerk must record the seal number on a chain-of-custody log for verification by the receiving election judges. The receiving election judges must verify the ballot container seal number before issuing ballots.

(c) When election judges are actively issuing ballots, the unvoted ballots must be in clear view of a minimum of two election judges of different party affiliations and one of the election judges must actively monitor the ballots unless the ballots are stored in a locked location accessible only to election officials.

(d) A minimum of two election judges of different party affiliations must reconcile and document all unvoted, issued, and spoiled paper ballots at the end of each day the polling center is open and immediately report any inventory discrepancies to the county clerk.

(e) If unvoted paper ballots are stored overnight at the polling location, the ballots must be sealed in containers and stored in a locked location accessible only to election officials.

20.7.2 Voted ballots

(a) Voted ballots may only be handled by the following individuals:

(1) County clerks;

(2) County clerk staff engaged in the performance duties for the county clerk;

(3) Election judges from the time ballots are returned until all required or requested recounts have concluded; and

(4) Canvass board members sworn under oath from the time ballots are returned until all required or requested recounts have concluded.

(b) When ballot processing is not actively occurring, the designated election official must seal and store ballots and opened and unopened return envelopes in a secure ballot area.

(c) Transportation of ballot boxes with voted ballots from VSPCs and ballot drop boxes to central count facilities:

(1) A bipartisan team, of election judges and/or staff, must seal all ballot boxes that contain voted ballots so that no person can access the ballots without breaking a seal. The team must record all seals in the chain-of-custody log, verify that the required seals are intact, and sign and date the log.

(2) A bipartisan team, of election judges and/or staff, must accompany all ballot boxes that contain voted ballots at all times except when the ballot box is located in a vault or secure physical location.

20.7.3 Remedies

(a) In the event that a county clerk discovers that a violation of Rule 20.7 has occurred, they must file an incident report required by Rule 20.12.2(a).

(b) The Department of State may take any action under Rule 20.12.2(b) to remedy a violation of Rule 20.7.

20.8 Security for voting system providers and vendors

20.8.1 Remote election programming services

(a) A county clerk may not install or import into its voting system an election database or project programmed or created by the voting system provider using voting system components other than those owned or leased by the county and situated in the county's secure elections facility.

(b) Rule 20.8.1(a) does not apply if the voting system provider first affirms on a form provided by the Secretary of State that:

(1) At all times during the election database or project programming, the voting system provider used only hardware and software certified for use in Colorado, as configured and verified during trusted build by the Secretary of State;

(2) At all times after installation of trusted build, the voting system provider operated all hardware utilized to program the election on a closed network and did not connect the hardware to the internet or any internet-connected device;

(3) At all times during the election programming process, the voting system provider complied with the security protocols for removable storage devices in Rule 20.5.3(c); and

(4) The voting system provider physically delivered to the county clerk removable storage media containing the finished election database or project and did not transmit using any method connected or exposed to the internet.

20.8.2 Voting system component replacement or repair

(a) A county clerk that sends a voting system component to a voting system provider for repair must submit an incident report to the Department as required by Rule 11.7.2 and an equipment acquisition/disposal form to the voting systems team at the Department.

(b) When the county clerk receives the repaired component, or receives a replacement component, the county clerk must verify the serial number on the component and seal numbers on the shipping container match the numbers listed on the trusted build affidavit included in the container, or if that is not possible, must arrange with the Department to have trusted build installed on the component. The county clerk must also submit a completed acquisition/disposal form to the Department at the time it receives the equipment before it can be used in any capacity during an election.

(c) If equipment is repaired by a vendor on-site, the county clerk must keep a maintenance log for the device that must contain the following:

(1) The model number, serial number, and the type of device;

(2) The software version, as applicable;

(3) The printed name and signature of the vendor repairing the equipment; and

(4) The date the vendor was on-site.

(d) A county clerk may not allow for the on-site repair or maintenance of a voting system component that has trusted build software installed except that a county may work with a voting system provider to replace a hard drive in a RAID configured voting system component on-site according to the published conditions of use for the voting system with the written approval of the Secretary of State.

(e) The county clerk or an election employee of the county clerk who is authorized to access a secure equipment area must escort the vendor's representative at all times while in a secure equipment area. At no time may the voting system vendor have access to any component of the voting system without supervision by the county clerk or an employee of the county clerk who is authorized to access a component of the voting system.

(f) Upon return of any voting system component sent for off-site maintenance, the county clerk must perform an acceptance test following the written procedures provided by the voting system vendor. The county clerk must maintain all documentation of the results of the acceptance testing on file with the specific device.

(1) If the maintenance was performed on a BMD, that BMD must be used to generate five ballots for use in the acceptance testing.

(2) If the maintenance was performed on a ballot scanner, then at least five ballots (a combination of BMD-generated ballots and non-BMD-generated ballots—at least one of each) must be tabulated on the scanner.

20.8.3 Remedies

(a) In the event that a county clerk or voting system provider discovers that a violation of Rule 20.8 has occurred, they must file an incident report required by Rule 20.12.2(a).

(b) The Department of State may take any action under Rule 20.12.2(b) to remedy a violation of Rule 20.8.

20.9 Security of other election systems

20.9.1 Statewide voter registration database (SCORE)

(a) SCORE username and password administration

(1) The SCORE customer support assigns county user administrator privileges to the individual designated in each county by the county clerk. The county clerk or election administrator must submit a request for county user administrator privilege to SCORE customer support in writing. The request must specifically state the full name of the county employee that is being assigned as a county user administrator.

(2) Each county is limited to two county user administrators, but a county clerk may apply to the Department for an additional county user administrator.

(A) The application must be submitted by the county clerk in writing to SCORE customer support and must state the full name of the county employee for which county user administrator privilege is being sought. The application must also state the specific reasons the county clerk is requesting the additional user administrator.

(B) SCORE customer support will notify the county clerk in writing whether the request is approved within five business days after receiving the application.

(3) The county user administrator is responsible for security administration and must assign all access privileges, as well as usernames and passwords for county employees and temporary election workers.

(A) For county employees, the county user administrator must assign a unique username in accordance with the naming conventions provided by the Secretary of State.

(B) Passwords must be assigned by the county user administrator upon initial authorization and must be changed by users and maintained confidentially.

(4) If a county employee or temporary election worker is no longer employed by the county, the county user administrator must immediately inactivate the username.

(b) SCORE network security requirements

(1) The county clerk must use only county-controlled access to networks with proper network security controls in place to access SCORE. The county may never use an open or shared public-use network to access SCORE.

(A) All wireless networks must meet the following minimum requirements:

(i) WPA2, or above, security must be enabled;

(ii) Shared wireless passwords or secrets must be changed every three months, at a minimum; and

(iii) Wireless keys must be a minimum of 14 characters in length and must include at least one number and mixed case letters.

(B) All networks must employ proper security controls to ensure malicious users cannot connect to the network, intercept SCORE communications, or otherwise attack the SCORE system. These controls must include, at a minimum, network firewalls and securely configured network equipment to prevent common attack mechanisms.

(2) All individuals who access the SCORE system must sign a SCORE Acceptable Use Policy (AUP) before the county provides a SCORE username.

(A) The county clerk, county SCORE user-administrator, and county elections IT manager, if applicable, must submit their signed AUP to the Secretary of State.

(B) The county clerk must retain the AUP for each individual who is assigned a SCORE username.

(i) The Secretary of State will audit the county AUP records for each county selected for annual inspection of its voting system maintenance records under Rule 20.12.1(a).

(ii) The Secretary of State will suspend access to SCORE for any individual whose AUP is not on file with the county clerk.

(3) If a government agency notifies a county clerk or if the county clerk otherwise knows of an attack, potential attack, or data breach on critical infrastructure in the clerk's office, SCORE, or any other county network or system that may impact the election or election equipment, the county clerk must notify the Secretary of State's office immediately using the contact information provided by the Secretary of State's office for this purpose.

20.9.2 Ballot-on-demand and mobile ballot production printers

(a) Software access, security, and storage

(1) The county clerk must change all Windows, and ballot-on-demand and mobile ballot production application passwords at least once per calendar year.

(2) Only election officials or authorized vendor representatives may operate the ballot-on-demand system or mobile ballot production printers.

(3) The county clerk may connect the ballot-on-demand or mobile ballot production laptop to an external network for the purpose of connecting to SCORE only if the county clerk maintains current virus protection, current operating system security patches, and implements firewalls to prevent unauthorized access.

(4) The county clerk must store the ballot-on-demand and mobile ballot production printer, laptop, and unused paper ballot stock in a locked storage area which is accessible only to election officials when the printer is not in use.

(5) The county clerk must ensure before use during an election that any wireless connectivity associated with a mobile ballot production printer or laptop or ballot-on-demand laptop is disabled.

(b) Ballot reconciliation

(1) The county clerk must reconcile ballots printed on demand in accordance with Rules 10.1.1 and 10.1.2.

(2) The county clerk must maintain damaged, misprinted, or unusable ballots as election records.

20.9.3 Remedies

(a) In the event that a county clerk discovers that a violation of Rule 20.9 has occurred, they must file an incident report required by Rule 20.12.2(a).

(b) The Department of State may take any action under Rule 20.12.2(b) to remedy a violation of Rule 20.9.

20.10 Retention and election project backups

20.10.1 Election project backup security

(a) To ensure election project backups have not been altered, a county clerk must store any media that contains an election project backup in a sealed container in a secure equipment area. The container must be sealed by at least one tamper-evident seal and have a chain-of-custody log.

(b) When accessing the sealed container containing any media that contains election project backups two election officials must verify the seal number(s) and sign and date the chain-of-custody log.

(c) Removeable media used to store election project backups must conform to the removeable media security standards in Rule 20.5.4(c). The media may only be connected to a component of a voting system with an intact trusted build.

(d) Any media that contains election project backups may not contain any data that is not exported by the voting system.

(e) Only employees of the county clerk's office that have passed a criminal background check according to Rule 20.2.1 may access any media that contains an election project backup, except any individual who is prohibited from having physical contact with any voting equipment under section 1-5-607(1), C.R.S., may not access any media that contains an election project backup.

20.10.2 Retention of voting system security records

(a) The county clerk must maintain all documentation of seals, chain-of-custody, trusted build, acceptance testing, transfer of equipment between parties, or any other documents related to the physical security of voting system components for 25 months after that component is no longer in the possession of a county.

(b) The county clerk must maintain the following as election records under section 1-7-802, C.R.S.:

(1) Access logs to secure ballot and secure equipment areas;

(2) Access logs for voting system component access;

(3) Video footage created under Rule 20.4.2;

(4) Election project backups required to be made under Rule 11.4.1(a), (b), (d), and (e);

(5) Logs generated by the election management system software of the voting system if those logs are not contained in the election project backup. This does not include logs generated outside of the election management system software; and

(6) Any other documents created by the county clerk to ensure the physical security of the voting system.

(c) All written entries in logs and other documentation must be in permanent ink and legible.

20.10.3 Remedies

(a) In the event that a county clerk discovers that a violation of Rule 20.10 has occurred, they must file an incident report required by Rule 20.12.2(a).

(b) The Department of State may take any action under Rule 20.12.2(b) to remedy a violation of Rule 20.10.

20.11 Security of operations

20.11.1 Contingency plans

(a) The county clerk must develop emergency contingency plans for voting equipment and voting locations in accordance with this Rule.

(b) In the event of a serious or catastrophic equipment failure, or when equipment is removed from service, or there is not adequate backup equipment to meet the requirements of section 1-5-501, C.R.S., the county clerk must notify the Secretary of State that the county clerk is using provisional ballots as an emergency voting method.

(c) The county clerk contingency plans and evacuation procedures must address emergency situations including fire, severe weather, bomb threat, civil unrest, electrical blackout, equipment failure, and any other emergency situations the county clerk identifies.

(d) The county clerk must develop procedures to address failures of SCORE continuity, which includes:

(1) Network failure,

(2) Power failure that lasts less than one hour, and

(3) Power failure that lasts more than one hour.

(e) At least one BMD in each voter service and polling center must have a backup battery, or be connected to an uninterruptible power supply, sufficient to sustain continuous operation for a minimum of two hours in the event of power loss.

(f) The county clerk must develop contingency plans which address an unexpected outage of any required video surveillance. The plan must include regular intervals at which the county will confirm that all required video surveillance is operational.

20.11.2 Closure of VSPCs due to emergency condition

(a) If as a result of an extreme weather event, natural disaster, act of God, human made incident, or disruption to, or threat of disruption to critical infrastructure, a county government or other entity closes all day, closes early, or delays the opening of a building where a voter service and polling center is located, then the county clerk may close for the day, close early, or delay the opening of any voter service and polling center located in those buildings affected.

(b) The county clerk must immediately notify the Secretary of State and the public of any closure or delayed opening of a voter service and polling center under this Rule.

(c) A county clerk must relocate VSPC operations to a backup location in the event a closure would result in the county not meeting their statutory minimum VSPCs. A county clerk must immediately notify the Secretary of State of the backup location that they will relocate to.

(d) The Secretary of State may petition a court under section 1-7-101 (1)(b), C.R.S., to extend the polling hours in a county or statewide if voter service and polling centers are closed or delayed opening under this Rule.

(e) If a county clerk closes or delays the opening of a voter service and polling center under this Rule, then the Secretary of State and county clerk must issue an emergency ballot available under section 1-7.5-115, C.R.S., to any voter who requests it due to the delay or closure.

20.12 Secretary of State inspections and remedies

20.12.1 Inspections

(a) A county clerk must make available to the Secretary of State, upon request, county documents and equipment, including, but not limited to:

(1) County maintenance records;

(2) Chain-of-custody logs;

(3) Trusted build integrity;

(4) Wireless status;

(5) Virus protection status;

(6) Password status (Bios, operating system, and applications);

(7) Access logs;

(8) Background check documents;

(9) Signed acceptable use policy agreements; and

(10) Video surveillance.

(b) In addition to the documentation listed in Rule 20.12.1(a), the county clerk must make all documentation related to the voting system and for every device used in the election available for Secretary of State inspection.

20.12.2 Remedies

(a) Incident report

(1) If a county clerk discovers or determines that a violation of any provision of Rule 20 has occurred, they must file an incident report with the Department of State as soon as feasible following the incident. The incident report must

describe in detail the incident and the rule that may have been violated and any other information the Department may require.

(2) After an incident report is filed under this Rule, the Department will investigate and determine what additional action or information, if any, is required.

(3) A county clerk must cooperate with the investigation of a violation of Rule 20. This includes providing any documentation or answers requested by the Department during the course of the Department's investigation.

(4) Based on the information gathered, the Department may take further action, including but not limited to, those actions described in Rule 20.12.2(b) to remedy the violation and to ensure future compliance with Rule 20.

(5) A county clerk's intentional failure to file an incident report required by this Rule or failure to cooperate with an investigation conducted by the Department of State may also result in any of the remedies listed in Rule 20.12.2(b).

(b) Remedies

(1) Upon discovering and investigating a violation of Rule 20, the Department may require a county clerk to take further action to remedy any violation and ensure future compliance with Rule 20.

(2) Any violation of Rule 20 may result in the prohibition or limitation on the use of, as well as decertification of, a county's voting system or components in accordance with section 1-5-621, C.R.S., and Rule 21.7.3.

(3) In the event that the Secretary of State determines that an election official has shown a serious or patterned failure to comply with any security requirements found in statute, these rules, the conditions of use of the voting system, or the acceptable use policy agreement for the voting system, the Secretary of State may take any or all of the following actions, including but not limited to:

(A) Requiring the county clerk to submit a security remediation plan no later than 90 days before the next election outlining the procedures the county clerk will follow to ensure compliance with the security requirements that were not followed;

(B) Prohibiting or limiting the use of, as well as decertification of, a county's voting system or components in accordance with section 1-5-621, C.R.S., and Rule 21.7.3;

(C) In accordance with section 1-1.5-104(2)(a)(II), C.R.S., appointing observers at the county expense to be present with the county clerk to ensure compliance with the security requirements; or

(D) Referring the matter to the Attorney General or District Attorney for potential investigation and prosecution under section 1-13-114, C.R.S., or any other applicable provision.