NORTH CAROLINA
State Board of Elections & Ethics Enforcement

*Mailing Address*:
P.O. Box 27255
Raleigh, NC 27611-7255

Phone: (800) 522-4723
Fax: (919) 715-0135

# NUMBERED MEMO 2018-12

**TO:** County Boards of Elections

**FROM:** Kim Strach, Executive Director

**RE:** Security Preparations

**DATE:** October 2, 2018

This Numbered Memo summarizes directives regarding certain devices and data handling ahead of early voting and Election Day. Please share this Numbered Memo with your county I.T. office and work closely with them to ensure appropriate implementation of these procedures and compliance with your county's particular I.T. policies.

## LAPTOPS

Laptops may contain critical security information, including SEIMS access and proxy/VPN access that allows the laptop to access county networks remotely. It is critically important that CBEs secure those laptops.

### LIMITING ACCESS

- **Login credentials must be traceable to individuals.** CBEs shall limit access to authorized persons. Laptop login credentials must vary (you may not have one username/password or generic usernames/passwords for all laptops).
- **Shorten screen lock-out times.** Set short screen lock times. Lock down the workstation with a short timeout period to ensure that computers or laptops are not accessible when not currently in use.
- **Logout when unattended.** Prior to leaving a laptop unattended, the laptop must be logged out and locked down to prevent unauthorized access.
- **Block remote access.** Remote access to laptops with SOSA or any SEIMS application is not permitted. This means that you may not give another person the ability to access SOSA or a SEIMS application from another computer.
- **Secure laptop locations.** Laptops shall not be left unattended in public spaces. All locations with laptops must be locked unless attended by CBE staff or elections officials.

## SECURING DATA

- **Encrypt hard drive.** You must encrypt the entire hard drive on any laptop containing SOSA software or other SEIMS programs. Encryption helps ensure data is secure if the laptop is stolen, returned, or recycled without proper wiping.
- **Follow county I.T. policies.** Comply with all applicable county information technology computer or laptop policies and procedures.

## THIRD-PARTY ACCESS

- **Block remote access.** Under no circumstances may the CBE authorize remote access or control by any third party or vendor to any system or device that contains a SEIMS application. Remote access includes but is not limited to desktop control, drag-and-drop file transfer and any connection that authorizes a third party to control a device with SOSA or any SEIMS application loaded, or which will have SOSA or any SEIMS application loaded.
- **Protect access by agreement.** Some counties rent laptops rather than maintain their own stock for precincts and early voting. Any use of a third-party laptop service must:
    1) be covered by data protection/confidentiality agreements approved by your county attorney;
    2) provide for the encryption of all devices;
    3) provide for the destruction of all data once the device is returned;
    4) ensure adherence to all policies contained in this Numbered Memo.

## NETWORK CONNECTIVITY

- If network connectivity is required to any State election server, that communication pathway must be secured by either:
    - A point-to-site encrypted VPN from the device to the network location of the state election server; or
    - A site-to-site VPN, which may be used only if the SOSA laptops are the ONLY devices on the network site connecting to the site with the state election server.
- If network connectivity is required at the site with SOSA installed, counties should opt for a wired connection. Wireless connectivity is only allowed if SSIDs are NOT broadcasted, strong passwords are used, and wireless encryption is implemented.

## TRACEABILITY

- Ensure SOSA usernames trace to one (and only one) SOSA user. Sharing user accounts and generic user accounts are prohibited.

### CLEARING DEVICES AFTER ELECTION

- Desktops and laptops with SOSA or other electronic poll book data installed shall be properly erased after each election, unless they are needed for an investigation. If these devices need to be retained, they must be physically secured and the chain of custody maintained. CBEs must ensure compliance with any directive of the State Board Office regarding retention of desktops and laptops, as that data could become important to an investigation.
- Portable data storage devices (ex. USB sticks) should not be recycled.

## USB STICKS

USB sticks and any device connected to voting equipment and laptops should be securely maintained. The below guidance addresses the use of USB sticks during the coming election and thereafter:

### MOCK ELECTION

- Counties should need only one USB drive to transfer all files from your Unity PC to SEIMS for the Mock Election. Perform your logic and accuracy (L&A) testing as instructed and generate all files/reports (ASCIIs, Block Style Reports, etc.—you will need to rename them appropriately), which may then be copied onto a single USB drive.

### ONE-STOP:

- Best practice is to use one USB drive per SOSA machine per day to transfer data from the site to the office. At minimum, you will need one USB drive per site to transfer data back out to those SOSA machines.

### ELECTION NIGHT:

- On Election Night you will need several USB drives, one for each ASCII file you transfer to your SEIMS workstation to import into Election Reporting. How many such transfers you perform will depend on many factors, but you must be sure to use a clean USB drive each time.

### AFTER YOU HAVE USED THE USB DRIVE:

- Do not delete the data on the USB drive.
- Place the USB drive in a coin envelope, write the precinct or voting location, and then sign, date, and seal the envelope. You may use pre-printed labels for this purpose.
- For Mock Election Records:
    - The USB drive has become a "record of machine testing" and thus falls under the category of "VOTING MACHINE LISTS, TESTING RECORDS, AND CERTIFICATIONS" for the purposes of records retention:

        - a) Destroy in office inventories, warranties, and registration data after the voting systems are no longer in use and have been disposed of as authorized by the SBE.
        - b) Destroy certifications and machine testing related records 5 years after the certification of the election the machine was tested for.
        - c) Destroy in office remaining records when superseded or obsolete.

- For Election Night and One Stop records:
    - The USB drive is now considered an "list documenting registered electors and votes cast" and thus falls under the category of "POLL LIST/REGISTRATION LIST/ROSTER/AUTHORIZATION TO VOTE (ATV)" for the purposes of records retention:
        - FEDERAL ELECTION: Destroy in office **22 months** after certification records concerning a primary, general, or special election involving federal offices.
        - NON-FEDERAL ELECTION: Destroy in office **2 months** after certification records concerning a primary, general, or special election not involving federal offices.

- When the USB drives meet their retention requirement date, delete all data from and reformat the drives. Best practice is to destroy all records that have met their retention requirements at the same time. If you choose not to destroy the USB drives, it is necessary to securely wipe the data on that drive before repurposing a stick for non-election purposes (this may require reformatting and other measures). USB drives cannot be reused for voting processes.

## PAPER POLL BOOK BACKUPS ELECTION DAY

Counties are to maintain paper poll book back-ups on Election Day in case electronic poll books fail. This scenario occurred in one of our counties in 2016 and some precincts did not have a paper poll book. Staff had to undertake emergency measures to deploy needed paper back-ups across the county on short notice and under difficult circumstances.

## STYLUS FOR TOUCH-SCREEN VOTING MACHINES

It remains best practice for all counties using touch-screen voting machines to provide a stylus for use by the voter. Styluses must be purchased off the shelf. Alternatively, the eraser end of unsharpened pencils has been used as a cost-effective means to help ensure voters' selections are recorded without incident.

## REQUIRED CYBERSECURITY TRAINING

Cyberattacks represent a very real threat to the integrity and transparency of our elections. Protecting against online threats begins with understanding how these attacks occur and protecting ourselves from these attacks. It is critical that every employee understand cybersecurity and how to protect themselves and their office from attack.

Our Agency is instituting a mandatory online security awareness training program for all employees at county boards of elections. Our security awareness training will be provided by Security Mentor (www.securitymentor.com), in conjunction with the training department of the NC State Board of Elections and Ethics Enforcement. The training is easy to access, completely web-based, and is relevant, fun, and interactive.

All county directors and staff of county boards of elections must complete this training prior to the beginning of one-stop early voting. If you have not provided staff information requested by Ted Fitzgerald, please do so no later than **Thursday, October 4th at noon**. The training department will provide more detailed information on when and how to access the training modules in a separate email after the Thursday deadline.

Together we will do everything possible to secure our elections. Thank you for your commitment.