System Security Specification Requirements

URCVT v.1.2.0 07-NY System Security Specification Requirements v.1.0.0 document is solely for use in the State of New York. This document can be expanded or updated as is necessary or required. Any recommendations listed in this document should not supersede user jurisdiction procedures or other controlling governance entities. Attached as an appendix to this document is the New York State Board of Elections Certified Voting System Security Policy, which is to be relied upon in cases where more information is required.

URCVT v.1.2.0 07-NY System Security Specification Requirements v.1.0.0

V.2:2.6 System Security Specification
Vendors shall submit a system security specification that addresses the security requirements of Volume I, Section 7. This specification shall describe the level of security provided by the system in terms of the specific security risks addressed by the system, the means by which each risk is addressed, the process used to test and verify the effective operation of security capabilities and, for systems that use public telecommunications networks as defined in Volume I, Section 6, the means used to keep the security capabilities of the system current to respond to the evolving threats against these systems.

Information provided by the vendor in this section of the TDP may be duplicative of information required by other sections. Vendors may cross reference to information provided in other sections provided that the means used provides a clear mapping to the requirements of this section. Information submitted by the vendor shall be used to assist in developing and executing the system certification test plan. The Security Specification shall contain the sections identified below.

V.2:2.6.1 Access Control Policy
The vendor shall specify the features and capabilities of the access control policy recommended to purchasing jurisdictions to provide effective voting system security. The access control policy shall address the general features and capabilities and individual access privileges indicated in Volume I, Subsection 7.2.

- Access to the Universal Ranked Choice Voting Tabulator (UCRVT) should be at minimum made by no less than 2 bipartisan employees within the user jurisdiction. These employees should have received the suggested training time provided by the vendor before accessing the software. See ***URCVT v.1.2.0 10-NY Personnel Deployment and Training v.1.0.0*** for more***.***
- Access to the desktop or laptop should require password entry from the initial operating system for all users assigned to operate the URCVT. See ***URCVT v.1.2.0 16-NY System Hardening Procedures v.1.0.0*** document for more information.
- Employees accessing the software should be provided a paper log tracking for the purposes of establishing a recorded access record. The log should require the name of

the personnel accessing the system, purpose of access, and the start and end times. This log should be maintained as part of the official election record and for as long as the user jurisdiction is required to maintain records per their controlling records retention schedule.

- The software provides full capabilities and access upon start up and the vendor recommends not less than two bipartisan user employees access the system simultaneously to prevent incorrect, accidentally or on purpose, use of the features to tabulate ranked-choice voting results.

V.2:2.6.2 Access Control Measures

The vendor shall provide a detailed description of all system access control measures and mandatory procedures designed to permit access to system states in accordance with the access policy, and to prevent all other types of access to meet the specific requirements of Volume I, Subsection 7.2. The vendor also shall define and provide a detailed description of the methods used to preclude unauthorized access to the access control capabilities of the system itself.

- The URCVT software employs a single user level and the user has access to the capabilities of the software described in the ***URCVT v.1.2.0 300-NY Configuration File Parameters v.1.0.0*** document and described by the ***URCVT v.1.2.0 08-NY System Operations Procedures v.1.0.0***. The vendor recommends that at least two users visually observe the software during use.
- Access to the Universal Ranked Choice Voting Tabulator (UCRVT) should be at minimum no less than 2 bipartisan employees within the user jurisdiction. These employees should have received the suggested training time provided by the vendor before accessing the software. See ***URCVT v.1.2.0 10-NY Personnel Deployment and Training v.1.0.0.***

V.1:7.2.1 General Access Control Policy

a. The vendor shall specify the general features and capabilities of the access control policy recommended to provide effective voting system security. Although the jurisdiction in which the voting system is operated is responsible for determining the access policies for each election, the vendor shall provide a description of recommended policies for: Software access controls

- The URCVT software employs a single user level and the user has access to the capabilities of the software described in the ***URCVT v.1.2.0 300-NY Configuration File Parameters v.1.0.0*** document and described by the ***URCVT v.1.2.0 08-NY System Operations Procedures v.1.0.0***. The vendor recommends that at least two users visually observe the software during use.
- Access to the Universal Ranked Choice Voting Tabulator (UCRVT) should be at minimum no less than 2 bipartisan employees within the user jurisdiction. These employees should have received the suggested training time provided by the

vendor before accessing the software. See ***URCVT v.1.2.0 10-NY Personnel Deployment and Training v.1.0.0.***

b. Although the jurisdiction in which the voting system is operated is responsible for determining the access policies for each election, the vendor shall provide a description of recommended policies for: Hardware access controls

- Maintaining proper physical security to all computers is absolutely essential. When the equipment is in use, no less than two bipartisan properly trained and trusted election officials should be present in the room with the equipment at all times. When the equipment is not being used (for instance, between elections), the computer and any backup hardware should be kept in a locked room, and entry to that room should be restricted and logged.

c. Although the jurisdiction in which the voting system is operated is responsible for determining the access policies for each election, the vendor shall provide a description of recommended policies for: Communications

- The ***URCVT v.1.2.0 System Hardening Procedures v.1.0.0*** requires users to turn off all networking features on hardware. No URCVT installed computer should ever run with its Wi-Fi enabled. No URCVT computer should ever be connected to any public network. For software installation, files should be captured to a USB flash drive using only secure methods. For more information see ***URCVT v. 1.2.0 System Hardening Procedures v. 1.0.0.***

d. Although the jurisdiction in which the voting system is operated is responsible for determining the access policies for each election, the vendor shall provide a description of recommended policies for: Effective password management

- Access to the desktop or laptop should require password entry from the initial operating system for all users assigned to operate the URCVT. Any additional user jurisdiction security requirements should also be maintained when accessing any user jurisdiction owned equipment.

e. Although the jurisdiction in which the voting system is operated is responsible for determining the access policies for each election, the vendor shall provide a description of recommended policies for: Protection abilities of a particular operating system

- The user jurisdiction is fully responsible for maintaining owned hardware in keeping with universal maintenance and security standards including all updates and security patches for the operating system in use. For more information see ***URCVT v. 1.2.0 System Hardening Procedures v. 1.0.0*** and ***URCVT v. 1.2.0 09-NY System Maintenance Procedures v. 1.0.0.***

f. Although the jurisdiction in which the voting system is operated is responsible for determining the access policies for each election, the vendor shall provide a description of recommended policies for: General characteristics of supervisory access privileges

- Access to the Universal Ranked Choice Voting Tabulator (UCRVT) should be at minimum no less than 2 bipartisan employees within the user jurisdiction. These employees should have received the suggested training time provided by the

vendor before accessing the software. See ***URCVT v.1.2.0 10-NY Personnel Deployment and Training v.1.0.0***

- The user jurisdiction is fully responsible for assigning access to the software and procuring the suggested training (see ***URCVT v.1.2.0 10-NY Personnel Deployment and Training v.1.0.0***) for those employees.
- The user jurisdiction is also responsible for creating and maintaining a segregation of duties plan and a backup plan where there will be no less than 2 bipartisan employees identified in the event that assigned personnel are unable to fulfill their assigned roles.

g. Although the jurisdiction in which the voting system is operated is responsible for determining the access policies for each election, the vendor shall provide a description of recommended policies for: Segregation of duties

- Access to the Universal Ranked Choice Voting Tabulator (UCRVT) should be at minimum no less than 2 bipartisan employees within the user jurisdiction. These employees should have received the suggested training time provided by the vendor before accessing the software. See ***URCVT v.1.2.0 10-NY Personnel Deployment and Training v.1.0.0***
- The user jurisdiction is fully responsible for assigning access to the software and procuring the suggested training (see ***URCVT v.1.2.0 10-NY Personnel Deployment and Training v.1.0.0***) for those employees.
- The user jurisdiction is also responsible for creating and maintaining a segregation of duties plan and a backup plan where there will be no less than 2 bipartisan employees identified in the event that assigned personnel are unable to fulfill their assigned roles.

h. Although the jurisdiction in which the voting system is operated is responsible for determining the access policies for each election, the vendor shall provide a description of recommended policies for: Any additional relevant characteristics

- There are no additional relevant characteristics associated with the URCVT.

V.1:7.2.1.1 Individual Access Privileges

a. Voting system vendors shall: Identify each person to whom access is granted, and the specific functions and data to which each person holds authorized access

- Access to the Universal Ranked Choice Voting Tabulator (UCRVT) should be at minimum no less than 2 bipartisan employees within the user jurisdiction. These employees should have received the suggested training time provided by the vendor before accessing the software. See ***URCVT v.1.2.0 10-NY Personnel Deployment and Training v.1.0.0***
- The user jurisdiction is fully responsible for assigning access to the software and procuring the suggested training (see ***URCVT v.1.2.0 10-NY Personnel Deployment and Training v.1.0.0***) for those employees.
- The user jurisdiction is also responsible for creating and maintaining a segregation of duties plan and a backup plan where there will be no less than 2 bipartisan

employees identified in the event that assigned personnel are unable to fulfill their assigned roles.

b. Voting system vendors shall: Specify whether an individual's authorization is limited to a specific time, time interval or phase of the voting or counting operations

- Access to the Universal Ranked Choice Voting Tabulator (URCVT) should be limited to no less than 2 bipartisan employees within the user jurisdiction.
- Upon startup the software provides capabilities described in the ***URCVT v.1.2.0 300-NY Configuration File Parameters v.1.0.0*** document and described by the ***URCVT v.1.2.0 08-NY System Operations Procedures v.1.0.0***. The vendor recommends that at least two users visually observe the software during use simultaneously to prevent incorrect, accidentally or on purpose, use of the features to tabulate ranked-choice voting results.
- Access to the URCVT should only be permitted during pre-election logic & accuracy testing and post-election tabulation of ranked-choice voting results from the voting system generated cast vote records (CVR).

c. Voting system vendors shall: Permit the voter to cast a ballot expeditiously, but preclude voter access to all aspects of the vote counting processes

- The URCVT does not have access to physical ballots or the voting system equipment used by voters to cast those ballots.
- The URCVT is used solely in the official facilities of the user jurisdiction. The vendor does not recommend the voter have any access to the software as installed by the user jurisdiction.

V.1:7.2.1.2 Access Control Measures

a. Vendors shall provide a detailed description of all system access control measures designed to permit authorized access to the system and prevent unauthorized access. Examples of such measures include: Use of data and user authorization

- Access to the Universal Ranked Choice Voting Tabulator (UCRVT) should be limited to no less than 2 bipartisan employees within the user jurisdiction.
- Upon startup the software provides capabilities described in the ***URCVT v.1.2.0 300-NY Configuration File Parameters v.1.0.0*** document and described by the ***URCVT v.1.2.0 08-NY System Operations Procedures v.1.0.0***. The vendor recommends that at least two users visually observe the software during use simultaneously to prevent incorrect, accidentally or on purpose, use of the features to tabulate ranked-choice voting results.
- Access to the URCVT should only be permitted during pre-election logic & accuracy testing and post-election tabulation of ranked-choice voting results from the voting system generated cast vote records (CVR).

b. Vendors shall provide a detailed description of all system access control measures designed to permit authorized access to the system and prevent unauthorized access. Examples of such measures include: Program unit ownership and other regional boundaries

- The user jurisdiction is fully responsible for assigning access to the software and procuring the suggested training (see ***URCVT v.1.2.0 10-NY Personnel Deployment and Training v.1.0.0***) for those employees.
- The user jurisdiction is also responsible for creating and maintaining a back up plan in the event that assigned personnel are unable to fulfill their assigned roles.

c. Vendors shall provide a detailed description of all system access control measures designed to permit authorized access to the system and prevent unauthorized access. Examples of such measures include: One-end or two-end port protection devices

- The URCVT software does not use any one-end or two-end port encryption devices.

d. Vendors shall provide a detailed description of all system access control measures designed to permit authorized access to the system and prevent unauthorized access. Examples of such measures include: Security kernels

- The URCVT software does not use security kernels.

e. Vendors shall provide a detailed description of all system access control measures designed to permit authorized access to the system and prevent unauthorized access. Examples of such measures include: Computer-generated password keys

- The URCVT software does not use computer-generated password keys.

f. Vendors shall provide a detailed description of all system access control measures designed to permit authorized access to the system and prevent unauthorized access. Examples of such measures include: Special protocols

- The URCVT software does not require special protocols as data does not transmit in or out via a web-based system.
- The vendor does recommend a dedicated USB flash drive and backup be secured with the hardware and used for no other purpose than software use.

g. Vendors shall provide a detailed description of all system access control measures designed to permit authorized access to the system and prevent unauthorized access. Examples of such measures include: Message encryption

- The URCVT does not require message encryption as data does not transmit in or out via a web-based system.

h. Vendors shall provide a detailed description of all system access control measures designed to permit authorized access to the system and prevent unauthorized access. Examples of such measures include: Controlled access security

- URCVT access takes place at a single central-count location. The software and hardware reside at this location. All election personnel are present at this location.
- Physical access to the site is controlled by policy and procedures under control of the jurisdiction.
- Physical access to the system hardware is controlled by policy and procedures under control of the jurisdiction.

- At no time should the hardware with installed software be connected to the internet via WiFi or ethernet. See ***URCVT v.1.2.0 16-NY System Hardening Procedures v. 1.0.0*** for more.
- The user jurisdiction is fully responsible for assigning access to the software and procuring the suggested training (see ***URCVT v.1.2.0 10-NY Personnel Deployment and Training v.1.0.0***) for those employees.
- The user jurisdiction is also responsible for creating and maintaining a back up plan in the event that assigned personnel are unable to fulfill their assigned roles.

V.2:2.6.4 Software Installation
The vendor shall provide a detailed description of the system capabilities and mandatory procedures for purchasing jurisdictions to ensure secure software (including firmware) installation to meet the specific requirements of Volume I, Subsection 7.4. This information shall address software installation for all system components.

V.1:7.4 Software Security
Voting systems shall meet specific security requirements for the installation of software and for protection against malicious software.

- See ***URCVT v.1.2.0 16-NY System Hardening Procedures v. 1.0.0*** for more information.

V.1:7.4.1 Software and Firmware Installation

a. The system shall meet the following requirements for installation of software, including hardware with embedded firmware. If software is resident in the system as firmware, the vendor shall require and state in the system documentation that every device is to be retested to validate each ROM prior to the start of election operations.

- Not applicable to the URCVT software.

b. The system shall meet the following requirements for installation of software, including hardware with embedded firmware. To prevent alteration of executable code, no software shall be permanently installed or resident in the voting system unless the system documentation states that the jurisdiction must provide a secure physical and procedural environment for the storage, handling, preparation, and transportation of the system hardware.

- The URCVT software shall only be installed during the election process and shall be removed after the completion of canvass (i.e., not permanently installed) and/or use the hardware security caveats.

c. The system shall meet the following requirements for installation of software, including hardware with embedded firmware. The voting system bootstrap, monitor, and device-controller software may be resident permanently as firmware, provided that this firmware has been shown to be inaccessible to activation or control by any means other than by

the authorized initiation and execution of the vote counting program, and its associated exception handlers.

- The URCVT files are software files only. There is no firmware.

d. The system shall meet the following requirements for installation of software, including hardware with embedded firmware. The election-specific programming may be installed and resident as firmware, provided that such firmware is installed on a component (such as a computer chip) other than the component on which the operating system resides.

- The URCVT does not require election specific programming to be created or installed. See **URCVT v. 1.2.0, 08-NY System Operations Procedures, v. 1.0.0** for more information.

e. The system shall meet the following requirements for installation of software, including hardware with embedded firmware. After initiation of election day testing, no source code or compilers or assemblers shall be resident or accessible.

- The application is only present in compiled form. After installation of URCVT users have no access to source code, compilers or assemblers. For more information see ***URCVT v. 1.2.0 14-NY Tabulator Build and Hashing Instructions v. 1.0.0***, ***URCVT v. 1.2.0, 16-NY System Hardening Procedures, v. 1.0.0*** and ***URCVT v. 1.2.0, 200-NY Installation Instructions for Universal RCV Tabulator - Windows OS, v. 1.0.0.***

V.1:7.4.4 Software Distribution

a. The vendor shall document all software including voting system software, third party software (such as operating systems and drivers) to be installed on the certified voting system, and installation programs.

- Software that must be installed on URCVT system:
  - Windows 10 Pro with the latest service pack installed
  - URCVT v. 1.2.0
  - Microsoft Excel
  - Notepad
  - Microsoft .NET Framework 3.8
  - Microsoft .NET Framework 4.5
  - Users must also retain access to:
    - Command Prompt
    - Digital Signature tools
    - Decryption tools
  - Optional anti-virus software
  - Optional UPS and printer drivers
  - See ***URCVT v. 1.2.0, 16-NY System Hardening Procedures, v. 1.0.0*** for more information.
- No other software is necessary for user operation of the URCVT.

a.i The documentation shall have a unique identifier (such as a serial number or part number) for the following set of information: documentation, software vendor name, product name, version, the certification application number of the voting system, file names and paths or other location information (such as storage addresses) of the software.

- Documentation, vendor name, product name, version, certification application number of voting system, and file names and paths are all referred to with unique labels in documentation and in the system itself. Also see ***URCVT v.1.2.0 13-NY Quality Assurance Plan v.1.0.0*** document for information about version numbers and documentation numbers.

a.ii The documentation shall designate all software files as static, semi-static or dynamic.

- All URCVT software files are static.
- All documentation, software vendor name, product name, version, certification application number, file names and storage paths, are all referred to by unique identifiers throughout documentation.
- For more information see ***URCVT v.1.2.0 13-NY Quality Assurance Plan v.1.0.0***
- ***URCVT v.1.2.0 02-NY Software Design and Specifications v.1.0.0***
- ***URCVT v.1.2.0 230-NY HashCode Instructions - Windows OS v.1.0.0***

V.1:7.4.6 Software Setup Validation

a. Setup validation methods shall verify that no unauthorized software is present on the voting equipment.

- The Installation guide ensures that only the authorized URCVT v. 1.2.0 software is present in the system through reliance on trusted build and hash code checks. For more information see ***URCVT v. 1.2.0 200-NY Installation Instructions for Universal RCV Tabulator - Windows OS v. 1.0.0***. Users also must set up their system according to the ***URCVT v. 1.2.0, 16-NY System Hardening Procedures, v. 1.0.0***, which will also verify that no unauthorized software is present on the voting equipment.

b. The vendor shall have a process to verify that the correct software is loaded, that there is no unauthorized software, and that voting system software on voting equipment has not been modified, using the reference information from the NSRL or from a State designated repository.

b.i The process used to verify software should be possible to perform without using software installed on the voting system.

b.ii The vendor shall document the process used to verify software on voting equipment.

b.iii The process shall not modify the voting system software on the voting system during the verification process.

- Following the installation guide (***URCVT v.1.2.0 200-NY Installation Instructions for Universal RCV Tabulator - Windows OS v.1.0.0***) ensures that only the authorized URCVT v. 1.2.0 software is present in the system through reliance on trusted build and hash code checks. For more information see ***URCVT v. 1.2.0 200-NY Installation Instructions for Universal RCV Tabulator - Windows OS v. 1.0.0***. Users also must set up their system according to the ***URCVT v. 1.2.0, 16-NY System Hardening Procedures, v. 1.0.0***, which will also verify that no unauthorized software is present on the voting equipment.

c. The vendor shall provide a method to comprehensively list all software files that are installed on voting systems.

- Software that must be installed on URCVT system:
  - Windows 10 Pro with the latest service pack installed
  - URCVT v. 1.2.0
  - Microsoft Excel
  - Notepad
  - Microsoft .NET Framework 3.8
  - Microsoft .NET Framework 4.5
  - Users must also retain access to:
    - Command Prompt
    - Digital Signature tools
    - Decryption tools
  - Optional anti-virus software
  - Optional UPS and printer drivers
  - See ***URCVT v. 1.2.0, 16-NY System Hardening Procedures, v. 1.0.0*** for more information.

d. The verification process should be able to be performed using COTS software and hardware available from sources other than the voting system vendor.

d.i If the process uses hashes or digital signatures, then the verification software shall use a FIPS 140-2 level 1 or higher validated cryptographic module.

d.ii The verification process shall either (a) use reference information on unalterable storage media received from the repository or (b) verify the digital signature of the reference information on any other media.

- All verification processes rely upon COTS software and hardware available from sources other than the voting system vendor. Verification processes require users to follow secure handling procedures from relevant governing authorities and can be performed according to the instructions in ***URCVT v. 1.2.0, 230-NY HashCode Instructions Windows OS, v. 1.0.0*** and **URCVT v. 1.2.0, 08-NY System Operations Procedures, v. 1.0.0.** All vendor processes rely upon SHA512 hashes.

e. Voting system equipment shall provide a means to ensure that the system software can be verified through a trusted external interface, such as a read only external interface, or by other means.

- Vendor verification processes rely upon COTS software and hardware available from sources other than the voting system vendor. Processes require users to rely upon trusted external sources of information, such as governing authorities providing Trusted Builds. Users must follow secure handling procedures from relevant governing authorities. Verification process can be performed according to the instructions in ***URCVT v. 1.2.0, 230-NY HashCode Instructions Windows OS, v. 1.0.0*** and ***URCVT v. 1.2.0, 08-NY System Operations Procedures, v. 1.0.0***. All vendor processes rely upon SHA512 hashes.

f. Setup validation methods shall verify that registers and variables of the voting system equipment contain the proper static and initial values.

f.i The vendor should provide a method to query the voting system to determine the values of all static and dynamic registers and variables including the values that jurisdictions are required to modify to conduct a specific election.

f.ii The vendor shall document the values of all static registers and variables, and the initial starting values of all dynamic registers and variables listed for voting system software, except for the values set to conduct a specific election.

- Values are provided in documentation. For more information see ***URCVT v1.2.0 11-NY L&A Testing v1.0.0***, ***URCVT v1.2.0 08-NY System Operations Procedures v1.0.0***, ***URCVT v1.2.0 300-NY Configuration File Parameters v1.0.0***, and ***URCVT v1.2.0 05-NY Acceptance Test Procedures v1.0.0***

V.1:7.5.1 Maintaining Data Integrity

Voting systems that use telecommunications to communicate between system components and locations are subject to the same security requirements governing access to any other system hardware, software, and data function.

a. Voting systems that use electrical or optical transmission of data shall ensure the receipt of valid vote records is verified at the receiving station. This should include standard transmission error detection and correction methods such as checksums or message digest hashes. Verification of correct transmission shall occur at the voting system application level and ensure that the correct data is recorded on all relevant components consolidated within the polling place prior to the voter completing casting of his or her ballot.

- The URCVT does not communicate between system components and does not directly impact voters or the ability to completely cast his or her ballot.
- For the purposes of using the Cast Vote Record (CVR) the assigned user jurisdiction personnel should follow all user jurisdiction policies when accessing

data from the vote counting system and maintain jurisdiction established chain-of-custody procedures when in use.

V.1:7.5.4 Shared Operating Environment

Ballot recording and vote counting can be performed in either a dedicated or non-dedicated environment. If ballot recording and vote counting operations are performed in an environment that is shared with other data processing functions, both hardware and software features shall be present to protect the integrity of vote counting and of vote data.

a. Systems that use a shared operating environment shall: Use security procedures and logging records to control access to system functions

- The URCVT does not operate in a shared operating environment.

b. Systems that use a shared operating environment shall: Partition or compartmentalize voting system functions from other concurrent functions at least logically, and preferably physically as well

- The URCVT does not operate in a shared operating environment.

c. Systems that use a shared operating environment shall: Control system access by means of passwords, and restrict account access to necessary functions only

- The URCVT does not operate in a shared operating environment.

d. Systems that use a shared operating environment shall: Have capabilities in place to control the flow of information, precluding data leakage through shared system resources.

- The URCVT does not operate in a shared operating environment.

V.1:7.5.5 Incomplete Election Returns

a. If the voting system provides access to incomplete election returns and interactive inquiries before the completion of the official count, the system shall: Be designed to provide external access to incomplete election returns (for equipment that operates in a central counting environment), only if that access for these purposes is authorized by the statutes and regulations of the using agency. This requirement applies as well to polling place equipment that contains a removable memory module or that may be removed in its entirety to a central place for the consolidation of polling place returns

- The URCVT operates separately from the voting system used in the counting environment. The URCVT does not operate in the counting environment including but not limited to polling places. Access, external or otherwise, is not required or permitted.

b. If the voting system provides access to incomplete election returns and interactive inquiries before the completion of the official count, the system shall: Design voting system software and its security environment such that data accessible to interactive queries resides in an external file or database created and maintained by the elections software under the restrictions applying to any other output report:

b.i The output file or database has no provision for write access back to the system

- The URCVT operates separately from the voting system used in the counting environment. There is no ability to write access back to the system.

b.ii Persons whose only authorized access is to the file or database are denied write access, both to the file or database, and to the system

- The URCVT operates separately from the voting system used in the counting environment. There is no ability to write access back to the system.

V.2:2.6.6 Other Elements of an Effective Security Program The vendor shall provide a detailed description of the following additional procedures required for use by the purchasing jurisdiction:

a. Administrative and management controls for the voting system and election management, including access controls;

- The user jurisdiction should assign and train employees as per the ***URCVT v1.2.0 10-NY Personnel Deployment and Training v1.0.0*** documentation. These employees should work in bipartisan pairs whenever accessing the hardware where the software is installed and during actual use of the software itself.

b. Internal security procedures, including operating procedures for maintaining the security of the software for each system function and operating mode;

- The user jurisdiction should assign and train employees as per the ***URCVT v1.2.0 10-NY Personnel Deployment and Training v1.0.0*** documentation. These employees should work in bipartisan pairs whenever accessing the hardware where the software is installed and during actual use of the software itself.
- The hardware containing installed software should be secured in a reasonably climate-controlled area with access being permitted and monitored through the use of signed access logs and in compliance with any of the user jurisdiction's own facility security policies.

c. Adherence to, and enforcement of, operational procedures (e.g., effective password management);

- The user jurisdiction should assign and train employees as per the ***URCVT v1.2.0 10-NY Personnel Deployment and Training v1.0.0*** documentation. These employees should work in bipartisan pairs whenever accessing the hardware where the software is installed and during actual use of the software itself.
- The user jurisdiction should only install the software on hardware that is not ever connected to the internet via WiFi or ethernet connections. See ***URCVT v1.2.0 16-NY System Hardening Procedures v1.0.0*** for more.
- The hardware containing installed software should be secured in a reasonably climate-controlled area with access being permitted and monitored through the

use of signed access logs and in compliance with any of the user jurisdiction's own facility security policies.

d. Physical facilities and arrangements; and

- The hardware containing installed software should be secured in a reasonably climate-controlled area with access being permitted and monitored through the use of signed access logs and in compliance with any of the user jurisdiction's own facility security policies.

e. Organizational responsibilities and personnel screening.

- The user jurisdiction should assign and train employees as per the ***URCVT v1.2.0 10-NY Personnel Deployment and Training v1.0.0*** documentation. These employees should work in bipartisan pairs whenever accessing the hardware where the software is installed and during actual use of the software itself.
- The user jurisdiction is responsible for contacting the vendor to procure the recommended number of hours of training as per the ***URCVT v1.2.0 10-NY Personnel Deployment and Training v1.0.0*** documentation. This training may be done virtually or in person.

This documentation shall be prepared such that these requirements can be integrated by the jurisdiction into local administrative and operating procedures.

V.1:7.7.3 Protecting Transmitted Data

The transmitted data, especially via wireless communications, needs to be protected to ensure confidentiality and integrity. Examples of election information that needs to be protected include: ballot definitions, voting device counts, precinct counts, opening of poll signal, and closing of poll signal. Examples of other information that needs to be protected include: protocol messages, address or device identification information, and passwords.

Since radio frequency wireless signals radiate in all directions and pass through most construction material, anyone may easily receive the wireless signals. In contrast, infrared signals are line of sight and do not pass through most construction material. However, infrared signals can still be received by other devices that are in the line of sight. Similarly, wireless signals can be transmitted by others to create unwanted signals. Thus, encryption is required to protect the privacy and confidentiality of the voting information.

a. All information transmitted via wireless communications shall be encrypted and authenticated--with the exception of wireless T-coil coupling--to protect against eavesdropping and data manipulation including modification, insertion, and deletion.

- The URCVT does not use wireless transmissions to transmit data.

  a.i The encryption shall be as defined in Federal Information Processing Standards (FIPS) 197, "Advanced Encryption Standard (AES)."

  - The URCVT does not use wireless transmissions to transmit data.

a.ii The cryptographic modules used shall comply with FIPS 140-2, Security Requirements for Cryptographic Modules.

- The URCVT does not use wireless transmissions to transmit data.

b. The capability to transmit non-encrypted and non-authenticated information via wireless communications shall not exist.

- The URCVT does not use wireless transmissions to transmit data.

c. If audible wireless communication is used, and the receiver of the wireless transmission is the human ear, then the information shall not be encrypted.

- The URCVT does not use wireless transmissions to transmit data.

Document Revision History

Date	Version	Description	Author
04/27/2021	1.0.0	System Security Specification Requirements	Rosemary F. Blizzard

Voting System Security Policy

40 North Pearl St., Suite 5
Albany, NY 12207
August 11, 2015
Version 3.0

Table of Contents

1. NEED FOR SECURITY POLICY AND APPLICABILITY OF POLICY

Voting systems can represent a high-value target to motivated individuals or groups who, given the proper circumstances, can attempt to alter the outcome of an election via manipulation of the process and participants, the voting system itself, or the election results. Additionally, and perhaps more importantly, even the suspicion of an altered or otherwise compromised voting system could cast doubt on an election outcome. Election transparency and public confidence in the confidentiality, integrity, accountability, and availability of the voting system and election process must be ensured. Sound security policies and procedures are therefore necessary to complement the protections built into the voting systems themselves.

1.1 Threats to Electronic Voting Systems

The requirements outlined within this security policy are designed to provide transparency and increased public confidence in NYS election systems by mitigating the risk associated with threats, which include but are not limited to:

- Election results destroyed or miscounted due to unintentional or malicious activity
- Lack of or destruction of a valid audit trail or accountability information
- Attacks on voter privacy and ballot security
- Voting system failures or slowdowns that inhibit or prevent voting
- Undetected voting system problems, such as mis-calibration or loss of results
- Voting system software or hardware flaws that can be exploited by attackers
- Fraudulent acts by insiders or outsiders
- Uncertified or unauthorized software and/or voting systems being used in an election
- Attempts to load malicious software onto voting systems
- Attempts to vote multiple times (ballot stuffing)
- Flawed, weak or non-existent security access controls, including physical and logical controls
- Attacks on underlying operating system software and configuration settings, or third-party software (databases) present on a voting system
- Attempts to violate voter privacy or damage election integrity
- Any attempt to alter the outcome of the election by attacking the voting system or election information

1.2 Purpose

This Voting System Security Policy defines the security requirements that shall be met for all voting systems when used in any election in New York State (NYS), either conducted or facilitated by a County Board of Election (CBOE). This policy shall be adhered to by the New York State Board of Elections (NYSBOE) and by each County Board of Elections (CBOE). This policy complements the State of NY Election Law, as well as Subtitle V of Title 9 of the Official Compilation of Codes, Rules, and Regulations of the State of New York, Parts 6209 and 6210.

This policy also serves as the foundation for CBOE-specific security procedures that will implement the policy requirements. This policy references specific security procedure templates that are listed in Appendix B and available from NYSBOE. These templates represent a baseline starting point for CBOEs and are designed to be added to, as necessary, to meet local needs, so long as the CBOE remains in compliance with this policy. All final CBOE security procedures shall be submitted to the NYSBOE for approval.

NYSBOE has developed this policy for the management and security of voting systems in order to ensure the following properties are present for all elections conducted in New York:

- *Confidentiality* – Voters can vote in private, and election information is only available to those with authorized access
- *Integrity* – Election information and voting systems are managed and maintained via approved processes and by authorized individuals
- *Availability* – Voting systems are available and operating properly throughout all election modes
- *Accountability* – Election-related events and actions are controlled and recorded, as needed, to determine which actions were taken by CBOE staff or any other election personnel, and when

The implementation of this policy will help to ensure that each of the above properties is present and preserved, on all voting systems and across all election modes. When considering a security policy and related security procedures for voting systems, it is important to consider the environment and nature of the use of these systems, as there are different security risks associated with the various election modes. While CBOE security procedures can be expanded to reflect local environments they must remain compliant with this policy.

1.3 Policy Scope

This policy applies to NYSBOE, CBOEs, and all personnel responsible for any aspect of conducting elections in which a NYSBOE-certified or authorized voting system (either precinct-based or central count) will be used. The policy applies to, but is not limited to, all county employees, contractors, election workers, contract voting system technicians,

and voting system vendors, or any other personnel who have a role in the maintenance or use of the voting system. The scope of this policy incorporates security for all NYSBOE-certified or approved voting systems and election management systems (EMS), as well as election information generated from such systems. This policy defines security requirements applicable during all election modes of voting system use, including:

- *Storage Mode* - where voting systems are received and placed in secure CBOE storage facilities
- *Pre-Election Mode* - where voting systems are configured and readied for use within a secure CBOE controlled environment
- *Election Mode* - where voting systems are used by voters at poll sites
- *Post-Election Mode* - where results are tabulated and election result information is gathered and ultimately archived
- *Transportation Mode* - where voting systems are transported from one location to another
- *Installation and Maintenance Mode* - where voting system software is installed and voting systems undergo routine, periodic maintenance procedures

Security requirements in this policy are derived from several official sources (see Appendix A), from best practices for security of voting systems, research into security practices in other states, certification testing, CBOE and general voting system usage feedback based on actual election use.

1.4 Voting System Components

Currently, these voting system components are covered by this policy:

- Precinct Based Optical Scanner (PBOS) Systems
- Central Count Optical Scanner (CCOS) Systems
- Election Management Systems (EMS)
- Ballot Marking Devices (BMDs)
- Closed networks and all associated network equipment
- All computers used on the closed network as servers or clients to support the EMS, and all peripheral devices attached to those computers
- All hardware and software used to support a closed network
- Physical keys used to access voting systems
- Access control credentials, including but not limited to user IDs, passwords, cryptographic key pairs, and security tokens
- Devices and software used to perform software validations

- All electronic media used by the voting system
- All election information generated during an election, including but not limited to:
  - Ballot configuration information
  - Election configuration data
  - Ballot images and ballot records
  - All paper ballots (voted, spoiled, and unused)
  - All generated reports
  - Audit data from all voting system components

2. ORGANIZATIONAL AND FUNCTIONAL RESPONSIBILITIES

This section describes the security requirements and responsibilities placed on NYSBOE, CBOE, and associated staff.

2.1 Role of NYSBOE

2.1.1 Authoritative Source for Voting System Software

NYSBOE will be the authoritative source for all software permitted to be installed on voting systems. Certified vendor software and all associated third-party software is maintained by NYSBOE as part of the NYS Certified Software Distribution and is available to CBOEs upon request.

NYSBOE will provide approved voting system configuration and software validation information to each CBOE when newly-certified systems, software, and configurations are available. NYSBOE will maintain software validation information that corresponds to each NYS Certified Software Distribution version.

2.1.2 Use of Uncertified Third Party Software

It is the responsibility of NYSBOE to ensure that additional third-party software, when introduced into the voting system, does not invalidate the voting system's certification. Any CBOE requests to install software not included on the NYS Certified Software Distribution must be made to NYSBOE to ensure the software does not invalidate the certified system. Any software or hardware to be added to the certified voting system shall be submitted to NYSBOE for approval via the Change Management Procedure prior to a CBOE installing it.

2.1.3 Policy and Procedure Maintenance

NYSBOE will maintain this security policy and all associated security procedure templates. Whenever approved changes are made to voting systems or relevant election processes, NYSBOE will update the policies and procedures as necessary.

NYSBOE will provide security procedure templates for each CBOE to further review and customize as necessary to meet their individual needs. NYSBOE recommended security procedures will take precedence over any suggested security procedures provided by voting system vendors. CBOE feedback on voting system policies and procedures templates will be incorporated by NYSBOE as appropriate. CBOEs will be responsible for updating their content-specific security procedures.

Security procedure templates are listed in Appendix B and are available from NYSBOE.

2.1.4 Compliance Auditing

NYSBOE will perform periodic CBOE audits to ensure that compliance with this policy is being maintained. NYSBOE will also review and approve all CBOE security procedures.

2.1.5 Support to CBOEs

NYSBOE will provide support to CBOE staff and will serve as a resource for any election system security incidents or issues. Specifically, NYSBOE's responsibilities will include, but are not limited, to the following:

- Guidance and assistance to CBOEs, as needed, related to security concerns
- Technical security support, including providing assistance with software validation
- Authoritative source for the NYS Certified Software Distribution
- Authoritative source for software validation information (hash codes)
- Certifying or authorizing new voting systems and modifications to existing systems
- Providing security procedure templates as listed in Appendix B
- Reviewing and working with counties to approve CBOE-specific, customized security procedures
- Providing improvements to security practices via feedback from CBOEs

2.2 Role of CBOEs

2.2.1 CBOE Ownership and Responsibilities

All voting systems in NYS are owned and maintained by each respective CBOE. Each CBOE is responsible for supporting and maintaining the voting systems and election information to be in compliance with this policy.

2.2.2 Development of CBOE Specific Security Procedures

The CBOE shall establish an organizational framework to initiate and control the implementation of voting systems information security within the CBOE. This framework will include but not be limited to responsibilities for completing and modifying, as necessary, the security procedure templates provided by NYSBOE that implement this policy.

Each security procedure listed in Appendix B shall be adopted by the CBOE. As per 6210 regulations, a copy of each CBOE's security procedures shall be filed with the State Board upon adoption by the CBOE Commissioners.

2.2.3 CBOE Change Management

Each CBOE shall establish a process for change management. Change management defines the CBOE process for supporting changes made to the voting systems under its control. Change management ensures that only authorized changes are made to voting systems and uses change logs and other records to document when changes have occurred. Additionally, the change management program helps to ensure that only software supplied by NYSBOE as part of the NYS Certified Software Distribution is present on each voting system.

The CBOE change management process shall be designed to ensure that this security policy is enforced throughout each mode of voting system usage.

2.2.4 Configuration Management

Each CBOE shall adopt a change management program that includes a defined associated configuration management process. Configuration management includes the mechanisms that will be used to keep track of certified or authorized voting system configurations. This CBOE program shall define the methods used by the CBOE to document the configuration of each voting system and all election information so that it is known at all times.

The CBOE configuration management process shall integrate with and utilize the NYSBOE asset management software as required by NYSBOE. The CBOE configuration management process shall ensure that each voting system is registered within the NYSBOE asset management software.

2.2.5 Election Systems Security Officers (ESSO)

Each CBOE shall designate two persons, in a bipartisan team manner, to serve in the role of Elections Systems Security Officers (ESSOs). The ESSOs will be responsible and accountable for ensuring that the requirements contained within this security policy are met through the development and adoption of CBOE-specific security procedures. In addition to the election commissioners, the ESSOs act as the primary points of contact at the CBOE for NYSBOE when critical election systems-management information must be communicated. The ESSOs will be responsible for activities that include but are not limited to:

- Providing a communications link between NYSBOE and the CBOE
- Receiving notification of all voting system maintenance activities and critical operating system or voting system application software upgrades that must be applied
- Notifying of any changes that affect the certification status of a voting system
- Ensuring the implementation, monitoring, and enforcement of this policy
- Developing CBOE-specific security procedures necessary to implement this policy
- Developing the security incident response plan

- Investigating and reporting to NYSBOE all alleged election information-security violations as per the security incident response plan
- Assuring that CBOE staff is sufficient in number and training to use and maintain all county voting systems as defined in this policy and to carry out their responsibilities

2.2.6 CBOE Staff Security Awareness Requirements

All CBOE staff shall understand that individual accountability is vital to the success of voting systems information security. CBOE staff shall understand and abide by the following:

- Physical access to any voting systems is strictly limited to fulfilling a business need. Physical access shall be limited to CBOE staff members who are functioning in an assigned role requiring such access.
- Logical access to all voting systems shall always be associated with a unique account or user-ID individually assigned to a specific user.
- Individuals who use the voting systems as part of their assigned role shall only be allowed access to the voting system data to which they are authorized.
- All voting system accounts and authentication credentials shall be assigned only to individual users and shall never be shared.
- CBOE staff and election workers understand that all actions taken when using the voting systems are recorded and audited.
- CBOE staff and election workers shall report all suspicious activity to the appropriate supervisors and follow the Security Incident Response Procedure as necessary. If suspicious activity is in the direct chain-of-command of the election worker (i.e., their supervisor) or CBOE staff, the election worker or CBOE staff shall directly report this activity, in confidence, to NYSBOE.

2.2.7 Contingency Planning

The availability of election information and the ability of voters to accurately and privately cast votes is critical. CBOEs must be prepared for voting system failures and outside events that can impact an election as per Part 6210 of Subtitle V of Title 9 of the Official Compilation of Codes, Rules and Regulations of the State of New York.

The CBOE shall develop a contingency plan that addresses how an election shall be configured, tested, conducted, staffed, and tabulated in the event of an unanticipated or unavoidable event. The contingency plan shall include resolution of issues at CBOE offices, equipment storage facilities, and poll sites. The CBOE contingency plan shall identify, at a minimum, an alternate site from which election management, administrative, or canvassing tasks can be conducted in the event the primary facility is unavailable or unusable.

The CBOE contingency plan shall also include procedures to follow for individual system failures and other conditions that may render some portion of the election systems unusable. This contingency plan shall provide for the continuous functioning of elections in the event of voting system failures.

Specifically, the plan shall address, at a minimum, the following scenarios:

- Any failure or loss of the voting system, including EMS, PBOS, CCOS or BMD during any mode of operation or use
- Failure or loss of any election information
- Poll site disasters, which include system failure, extended power failure, or physical site disruption
- Unavailability of facilities, ballots, or necessary supplies
- Unavailability of election workers, technicians, or other necessary/required staff
- Provisions and processes for conducting paper ballot hand-counted elections

A contingency plan template is listed in Appendix B and is available from NYSBOE.

2.2.8 Security Incident Response

Each CBOE shall develop a formal security incident response plan and related Security Incident Response Procedure. The procedures shall address responses to real or suspected security incidents for all modes of voting system usage. The security incident response plan will define the organizational (CBOE) actions to be taken when a real or suspected security incident occurs. The following shall be included in this plan:

- Procedures for notification of the appropriate CBOE staff
- Procedures for notification of NYSBOE
- Clear definition of members in the incident team, roles of each member (including which have the authority to act as decision makers), contact information for any potential resource, and communication channels, both within the team and to external entities (voting system vendors, NYSBOE, law enforcement, media, etc.)
- Procedures to secure the voting system in a separate area for later inspection and to prevent use of the device until the incident is completely resolved
- Procedures to handle a wide variety of potential election-system security incidents, including the steps to preserve election results and the system state for subsequent analysis
- Procedures on how to document and follow-up on the incident and any relevant symptoms and messages generated by the voting system
- A procedure that addresses how to respond to outside media requests and concerns

- Procedures that address the reporting of incidents, identification of underlying causes, problem resolution, and prevention of incidents from recurring

Any time a breach occurs or there is a suspected breach, such as a broken tamper-evident seal, the breach or suspected breach shall be recorded by the CBOE and a review conducted, pursuant to the pre-established security incident response. A determination shall be made, per the procedures, as to the usability of the voting system and when NYSBOE will be notified.

Security incidents shall be reviewed by appropriate CBOE personnel, and the ESSOs, to determine the level and severity and exposure. Copies of Election Day security incident report forms and trouble call logs shall be provided to the State Board within ten days of the election. Security incidents determined to be of a more serious nature shall be addressed (as per the security incident response plan) by the CBOE pursuant to their adopted procedures and shall subsequently be reported to the State Board as soon as practicable.

3. VOTING SYSTEM AND ELECTION INFORMATION SECURITY

3.1 Confidentiality, Integrity, Availability and Accountability Requirements

Electronic voting systems use and generate a variety of election information that shall be protected. Election information includes all paper ballots created for an election and all election result data produced. Election information that is created, acquired, or used as part of an election, shall be properly protected throughout its life cycle. All voting systems and election information shall be protected in a manner to ensure that confidentiality, integrity, availability, and accountability properties are provided and preserved during all modes of use.

Confidentiality is the ability to ensure that sensitive information is kept private, is only available to authorized parties, and is not subject to unauthorized disclosure. Election information that could possibly violate a voter's right to privacy shall be protected to provide confidentiality where needed. While all election-related data can eventually become public record, certain data shall be treated as confidential during creation and when in transit.

Integrity is the assurance of accuracy and reliability of election information and the voting systems used to process that information. Election configuration data and election result data integrity is vital for trust in the voting systems used to conduct elections.

Availability ensures that voting systems and election information will provide reliable, timely, and efficient access to voting systems by authorized individuals. Voting system availability during an election is an essential security property for a successful election.

Accountability refers to the ability to account for all actions taken to create an election and for all election information. CBOEs shall maintain and be able to provide sufficient audit records of all actions performed on each voting system in each mode of use.

3.2 Paper Ballot Security

The security of paper ballots (Election Day and absentee ballots) throughout the entire election process is a key component in overall election security. From pre-election periods when ballots are received by a CBOE to post-election, when they are stored securely at the conclusion of an election there is a need to ensure the ballot confidentiality, availability and accountability properties are preserved. At each phase of an election there exists a potential for ballot tampering therefore secure ballot storage and transportation is essential.

Each CBOE shall develop a Secure Ballot Handling Procedure that ensures ballots are managed securely across all phases of the election. This procedure should minimally address the following:

- Receipt of ballots from print vendors (even when the print vendor is the CBOE)
- Handling and storage of ballots prior to an election (including absentee ballots)

- Election day transportation, handling and storage of ballots
- Post-election transportation, handling and storage of ballots (including scanning and counting of ballots on central count systems)
- Post-election ballot archiving

All paper ballots used during an election, including undistributed ballots and ballots that have been voted/spoiled, shall be under the control and possession of CBOE staff or poll worker staff at all times. Voted ballots shall be under elections staff control as per Election Result Data & Security Pack Chain-of-Custody Procedures.

Voted ballots shall always be stored within a secure ballot storage container.

Each CBOE shall establish procedures to ensure that ballots are kept secured in a manner that associates the ballots with the voting system on which they were cast.

3.2.1 Precinct-based Voting System's Voted Paper Ballot Confidentiality and Integrity

Voter privacy protections and confidentiality requirements for Election Day paper ballots include the following:

- A sufficient number of privacy booths shall be available at each poll site and be properly positioned to ensure that all voters can vote in private throughout the day: Part 6210.19(b)(2)(b).
- Privacy sleeves shall be provided to voters with their respective ballot, to facilitate the confidentiality of the ballot.
- A sufficient number of privacy sleeves shall be available at each poll site to ensure that all voters will be provided one with their respective ballot.
- Voting systems and privacy booths shall be setup and arranged at the poll site per NYSBOE's approved floorplan or other site map, for efficient equipment layout.
- Voted paper ballots shall always be stored in a secure ballot storage container.
- Voted paper ballots shall remain under the control and possession of authorized personnel at all times.
- As per Election Day Poll Site Procedures, tamper-evident security seals shall always be used on all secure ballot storage containers.
- Voted paper ballots shall not be left where they are vulnerable to tampering or where tamper evident controls or locks are not in place.
- Voted paper ballots shall follow appropriate Election Result Data & Security Pack Chain-of-Custody Procedures whenever they are transported.

- The security pack and voted and spoiled ballots, as well as opened packages of unused ballots shall be returned to CBOE on election night after canvassing activities have been completed.

3.2.2 Central Count Voted Paper Ballot Integrity

- Voted paper ballots shall always be stored in a secure ballot storage container.
- Voted paper ballots shall remain under the control and possession of authorized personnel at all times.
- Voted paper ballots shall not be left where they are vulnerable to tampering or where tamper evident controls or locks are not in place.

3.2.3 Unused Paper Ballot Integrity

- Unused paper ballots shall always be stored and managed as per voting system storage requirements.
- All unused paper ballots shall be accounted for at the conclusion of an election.
- Unused paper ballots shall be protected from unauthorized access at all times.
- Unused paper ballots shall always be transported as per the Voting System Transportation Chain-of-Custody Procedure.

3.3 Election Data Security

3.3.1 Election Result Data Chain-of-Custody

Upon completion of election tasks, election result data shall be protected and controlled at all times by the Election Result Data & Security Pack Chain-of-Custody Procedure. This procedure ensures that the election result data is always maintained under strict poll worker and CBOE possession and control. The CBOE shall ensure that it clearly tracks and documents the possession and custody of this information at each stage of handling.

An election result data & security pack chain-of-custody form is required to be created or updated whenever election result data is stored or transported. This form contains all information corresponding to:

- Election result data generated upon the closing of the polls (result reports, ballots, materials, and documents)
- The removal of any election result data from the voting system
- The transportation of election result data from the poll site to the CBOE
- The transportation of election result data from the CBOE into permanent storage

Election result data shall be placed in a security pack or secure ballot storage container and shall remain there until the expiration of the period for challenging elections and for

as long as required by law and State Board Regulations, unless a court orders the release.

Whenever election result data is moved, it shall only be moved using approved secure storage receptacles with all locks and tamper-evident security seals in place. Election result data shall only be transported as per the Election Result Data & Security Pack Chain-of-Custody Procedure.

3.3.2 Election Result Data Chain-of-Custody Form

The election result data & security pack chain-of-custody form tracks:

- All voting system identification information which identifies the source of election result data
- Current status: storage, in use, being serviced, disposed, etc.
- The object's intended destination
- The location and serial numbers of all security seals and/or locks which protect access to the election result data, as per relevant security procedures
- Signatures of election staff charged with preparing the election result data
- Signatures of personnel responsible for transporting the election result data
- Signatures of Election Day poll workers responsible for any transfer of election result data at the end of the Election Day

3.3.3 Election Information Archiving

Certain election information is required to be preserved, protected, and stored minimally for a period prescribed by NYSBOE General Retention and Disposition Schedule Election Records Guideline. Information that shall be protected shall be exported from the generating source and maintained on media that has been shown to be reliable and to meet the data-retention requirements. The following list identifies election information required to be archived upon the conclusion of each election:

- All election configuration files, ballot definitions, and supporting data used in the preparation of the election for all contests, ballot styles, and election districts
- Audit data from all election modes (pre-election, election, and post-election)
- Pre-qualification and quarterly test results, reports, and inputs
- All Election Result Data
- Printed election results (reports and canvass reports)
- Voted, spoiled, and unused paper ballots
- Software Validation Information and results
- Assigned individual roles and respective accounts

3.3.4 Audit Log Requirements

County Boards of Elections are responsible for the management of all voting system generated audit data that results from an election.

Audit data from each mode of each election (including voting-software audit logs and operating-system audit logs) shall be transferred in its entirety from voting systems to alternate media that are then stored in a secure facility under CBOE secure control.

3.3.5 Media requirements

Media used to store audit data shall be properly labeled to associate the data with the election to which it relates. Write-once media shall be used in order to store data without loss of integrity. The media shall be stored under CBOE secure control with the proper environmental controls (temperature, humidity, etc.) as prescribed by the media vendor.

3.3.6 Election Security Pack Chain-of-*Custody*

In order to provide election inspectors with a single and secure source for seals, tags, relevant forms, keys, ballot storage, and other security-related documents, a Security Pack (or secure ballot storage container) shall be used. It is recommended that a pouch, portfolio, secure ballot storage container, or similar container be procured and clearly marked as a SECURITY PACK. This container shall have a means of itself being sealed, both when delivered to inspectors and after polls are closed, ready for return to the CBOE on election night. One security pack per scanner/BMD shall be sent to the poll site and used to return all election result data other than paper ballots. Voted paper ballots and opened packages of unused paper ballots shall be returned to the CBOE on election night in an approved secure ballot storage container or security pack that has a separate election results data & security pack chain-of-custody form. When election result data is transported, multiple Security Packs may be necessary.

3.4 Voting Systems Security

3.4.1 Voting System Removable Media Requirements

Voting systems shall be configured to encrypt and digitally sign all data that is written to removable media whenever such voting system features exist.

All removable media used in a voting system during an election shall be protected by tamper evident controls as per the Voting System Transportation Chain-of-Custody Procedure whenever it is outside the CBOE secure control.

All voting system locks and access controls shall be used as designed and according to relevant procedures to protect removable media.

3.4.2 Voting Systems Integrity Requirements

- Voting systems should be in CBOE secure control at all times. When voting systems cannot be stored in CBOE secure control, they shall be managed as per the Voting System Transportation Chain-of-Custody Procedure.
- Voting system locks and tamper evident security seals shall be used to protect access to sensitive areas whenever voting systems are outside of CBOE secure control.
- Whenever a voting system has been outside of CBOE Secure Control, or has not been transported as per the Voting System Transportation Chain-of-Custody Procedure, or cannot be otherwise accounted for, the voting system shall undergo the County Receipt Procedure and pre-qualification testing prior to being used in an election.
- Voting systems, when used during an election, shall only be transported as per the Voting System Transportation Chain-of-Custody Procedure.
- Anti-virus software shall be installed and used on all relevant voting system components at all times.
- Voting system physical access controls and logical access controls shall be enabled and used at all times as per relevant security procedures.
- Voting system integrity controls, including authentication, authorization, and digital signature features, shall be enabled and in use at all times as per relevant security procedures.
- The CBOE shall ensure that any voting system security features or processes recommended by the vendor are implemented, so long as they do not conflict with this policy.
- CBOEs shall adopt security procedures that restrict and document all access to all voting systems.

3.4.3 Voting System Software Integrity

- Software validation procedures (hash check) shall be performed as per quarterly and pre-qualification testing requirements.
- Software validation procedures shall be used whenever evidence of tampering or a security breach has occurred.
- Only software originating from the NYS Certified Software Distribution or other NYSBOE-approved software shall be present on a voting system at any time.
- COTS Central Count Scanners with permanently installed firmware must be contained in a secure physical environment (closed network), as per relevant procedures, to protect voting system software against unauthorized access.

- Tamper-evident security seals and locks shall be used, as per relevant procedures, to protect voting system software against unauthorized access.
- All changes to voting systems shall be managed as per the voting system's maintenance and change management requirements within this policy.

3.4.3.1 Voting System Availability Requirements

- Sufficient election supplies such as paper ballots, markers, and voting system consumables shall be stored and made available during election mode.
- All voting systems and election information shall be secured via locks, tamper-evident security seals, and as per relevant security procedures whenever voting systems are outside of CBOE secure control. Voting systems shall be properly maintained by CBOEs as per all required procedures.
- Election information shall be backed up as per relevant security procedures, and shall be managed in a manner that provides for recovery of the information as needed.
- Each CBOE shall maintain a contingency plan.

3.4.3.2 Voting System Accountability

- Voting systems shall be protected as appropriate in each election mode with physical and logical access controls as per relevant security procedures.
- During elections, voting systems shall only be transported to and from the CBOE facility as per the Voting System Transportation Chain-of-Custody Procedure.
- Voting system location and status shall be maintained in the NYS asset management software or CBOE equivalent application (e.g. MS Access DB, MS Excel).
- Voting system audit features shall be understood, enabled, and tested periodically.
- Voting system auditing capabilities shall be enabled, as needed, to be able to determine how an election was configured and who configured it.
- CBOEs shall maintain the protective counter values for each voting system as part of their asset management processes, and do so in the NYS asset management software. The protective counter value shall be documented for each voting system so that it is known at all times.
- CBOEs shall maintain logs that document task and staff assignments, time in and out, account and password changes, and other data necessary to document the use of voting systems.

3.5 Voting System Transportation

The CBOE shall clearly track the secure lifespan of each voting system throughout its many uses and travels during elections in any given county. The Voting System

Transportation Chain-of-Custody Procedure shall be followed whenever voting systems are in use during an election and not in CBOE secure control. When voting systems are transported for purposes other than an election, the voting system shall undergo the County Receipt Procedure and pre-qualification testing prior to being used in an election.

3.5.1 Tracking of Voting Systems

All voting systems shall be tracked by the CBOE in the NYS asset management software or CBOE equivalent application (e.g. MS Access DB, MS Excel) throughout the lifespan of the system. Tracking begins when each voting system is accepted into inventory, and is thereafter updated as the unit moves from the board of elections to and from a poll site, a training class, a voter outreach event, to and from service that is performed off-site by the vendor, or at any other time the device will be out of the CBOE secure control.

The voting system transportation manifest form shall be used whenever voting systems are out of CBOE secure control, and the information shall become part of the asset management tracking.

3.5.2 Voting System Transportation Chain-of-Custody

The Voting System Transportation Chain-of-Custody Procedure shall be used whenever a voting system is being used during an election and is out of CBOE secure control. Due to election logistics, it may not be possible for the Voting System Transportation Chain-of-Custody Procedure to ensure personal, physical possession and control by authorized personnel at all times, (i.e., there may be instances where voting systems will be delivered to poll sites without a person there to receive and claim possession). The Voting System Transportation Chain-of-Custody Procedure, however, shall be used to document and reflect the possession and control by authorized parties, and this shall be the goal whenever possible. CBOEs should strive to minimize situations where possession and control of voting systems cannot be maintained.

3.5.3 Voting System Transportation Manifest Forms

A number of forms will be necessary to ensure that each mode of a voting system's travels and/or use can be traced and ultimately posted to the voting system transportation manifest form. The voting system transportation manifest form will serve to track the round-trip travel of each unit, from and to the CBOE storage facility to poll site(s) or off-site vendor service site(s). The Security Seal Manifest document will serve to record all security seals and tags placed on each unit at the CBOE in preparation for use on Election Day and will provide spaces for election inspectors to confirm seals as intact and unaltered at the opening of polls. Additionally, the Security Seal Manifest will have spaces where inspectors can log security seals that need to be used during Election Day, as well as those that need to be used at the close of polls.

In order to provide election inspectors with a single and secure source for seals, tags, voting system transportation manifest forms, keys, and other security-related documents, a Security Pack shall be used. It is recommended that a pouch, portfolio, or similar container be procured and clearly marked as a Security Pack. This container shall have a means of itself being sealed, both when delivered to inspectors and after polls are closed, ready for return to the CBOE on election night.

During an election, whenever the Voting System Transportation Chain-of-Custody Procedure is used, the corresponding transportation manifest form is used to track:

- The unit serial or other identification numbers
- Current status: storage, in use, being serviced, disposed, etc.
- The unit's intended destination
- The location and serial numbers of all security seals and/or locks which protect access to the equipment's sensitive areas, as determined by vendor documentation and NYSBOE guidelines
- Signatures of CBOE staff charged with preparing and approving the unit for use
- Signatures of personnel responsible for transporting the unit
- Signatures of Election Day poll workers responsible for the device in the polling place throughout Election Day
- CBOE staff checking the voting system back into inventory after use in an election.

At each leg of a voting system's journey (e.g., to CBOE, from CBOE to poll site, from poll site back to CBOE, from CBOE to vendor for service, back to CBOE, etc.), the voting system transportation manifest form shall be signed, the seals/locks shall be checked to verify that they have not been tampered with, and the lock/seal number(s) on the device shall be compared to the form to confirm that the number(s) in place at each check point are the same as those originally affixed by the CBOE.

CBOEs are responsible for creating county-specific Voting System Transportation Chain-of-Custody Procedures that address all voting system transportation needs unique to the CBOE and/or accommodate local practices. During election mode, the voting system transportation manifest forms shall be completed and/or signed by:

- Bi-partisan CBOE team as security locks/seals are affixed and the security packet is prepared for delivery to a poll site
- Inspector team responsible for opening the polls
- Inspector team responsible for closing the polls
- Bi-partisan CBOE team as device is returned to inventory and CBOE custody and/or the security packet is returned to CBOE

When voting equipment is being transported for non-election events such as service or training, the Transportation Manifest Form shall be maintained as per the Voting System Transportation Chain-of-Custody Procedure.

The voting system transportation manifest form(s) ensures that control and possession at each leg of the device's journey can be documented. This form will be completed and signatures affixed by:

- CBOE inventory team
- Transport personnel
- Poll site personnel
- Vendor personnel
- Election inspector team responsible for opening and closing the poll site
- Training and outreach sessions

3.6 Voting System Maintenance

All changes to any voting system shall be made following current change management procedures. The following sections outline maintenance requirements.

All updates (e.g., operating system, anti-virus) and software installation shall be applied using vendor-prescribed procedures, logged in the equipment maintenance log, and performed by individuals authorized by the CBOE to perform that work. Any credentials (i.e., accounts, passwords, etc.) needed to perform the work shall be uniquely assigned to the individuals doing the work.

3.6.1 Operating System (OS) updates

No update shall occur to the Operating System (OS) of any voting system equipment, unless that update has been recommended by the voting system vendor and approved by NYSBOE. NYSBOE will distribute the update received from the vendor to the CBOEs. The CBOEs are prohibited from installing any software received directly from the vendor.

3.6.2 Software Installation and Updates

No update shall occur to the software of any voting system unless that update has been certified or authorized by NYSBOE. This includes updates to all software, including operating systems. Only software originating from the NYS Certified Software Distribution is permitted on each voting system.

3.6.3 Use of Anti-Virus

Anti-Virus (AV) software shall be installed and maintained as per vendor-prescribed procedures and according to NYSBOE policy and procedures. AV software is required to be present on all EMS systems (including servers and workstations, if that is how the

EMS is architected), Central Count workstations and may be required on other voting system components.

AV software updates may be installed on voting systems without NYSBOE approval or notification. AV software updates are not part of the NYS Certified Software Distribution and, therefore, each CBOE is responsible for validating the authenticity of the AV updates.

3.6.4 Voting System Operating System Hardening

All voting systems shall have undergone system hardening using the vendor-prescribed procedures and any additional procedures as necessary. System hardening is performed by the CBOE staff (with assistance from voting system vendors as needed) during the installation and configuration of new voting systems. There shall be no changes to the Operating System configuration on any voting system device (with the exception of those prescribed in vendor documentation and approved by NYSBOE) once the system has been hardened.

3.7 Voting System Software Validation

Before any voting system can be used for an election, the software on that system shall be either re-installed from the NYS Certified Software Distribution or validated to ensure that it is the same software certified or authorized by NYSBOE.

Validation shall be done using the software validation procedures created by the system vendor and approved by NYSBOE. Software validation is often called a "Hash Check," as the process examines the hashes [software fingerprint] of all software on the system and compares these to hash values provided by NYSBOE. Any failure or anomaly noted during the software validation process shall be considered a breach of security and shall be investigated using the Security Incident Response procedures created by the CBOE and reported to NYSBOE as soon as practicable. Software validation test methods shall utilize the most recent HASH values provided to the CBOE by NYSBOE.

Voting system software re-installations can only be done consistent with relevant security procedures and only from the NYS Certified Software Distribution.

3.7.1 Software Validation Testing Requirements

Software validation testing or software re-installation from the NYS Certified Software Distribution shall always occur as part of each Pre-Qualification Test.

Software validation testing or re-installation shall occur as part of quarterly testing whenever:

- The security incident response plan has been invoked for the device. Note: The incident response plan shall be invoked if there is a broken or missing seal or if the tamper-evident seal number does not match the number on relevant reports or forms. The device cannot be used until the investigation has been completed.

- Maintenance has been performed on the device since the last software validation check, including any software or firmware modifications.
- There is any evidence of tampering with a voting system, including but not limited to:
  - Missing or damaged seals or locks
  - Seals or locks that appear to have been tampered with
  - Seal numbers that are inconsistent with the last voting system transportation chain-of-custody log entry

3.7.2 Use of Non-certified Voting System Software

Software, other than AV updates, that was not part of the NYS Certified Software Distribution or authorized by NYSBOE, shall not be installed on any voting system. If such software (i.e., utility software, backup software, new AV software) is deemed necessary, then such software shall be recommended by the voting system vendor or requested by the CBOE via the Change Management Procedure and tested and approved for use by NYSBOE.

3.7.3 Use of COTS Central Count Scanners

Firmware on the COTS Central Count Scanners cannot be removed by the CBOE, and thus is considered "permanently installed." There must be physical and procedural protections of the scanning device and the County/jurisdiction must provide a secure physical environment along with following the NYSBOE security procedures for using a central count system. If the physical and procedural protections are properly adhered to for the central count scanners, this will compensate for the inability to conduct a hash check.

3.8 EMS and Central Count Voting System Requirements

As part of the certification of voting systems for use in New York State, the EMS and central count voting system is tested and certified on the hardware platform and software provided by the voting system manufacturer. The software is designed to perform only election-management functions and must exactly match the software specifications of the certified platform.

CBOE EMS and central count voting system hardware platforms shall comply with the vendor specifications.

Although it is feasible to purchase and use system hardware from a source other than the voting system manufacturer, the system shall meet and be configured to the same exact specifications as the vendor's voting system requirements. This means that all voting system software present on the EMS and central count voting system must exactly match the certificated versions and be installed from the NYS Certified Software Distribution. When a CBOE chooses to provide their own EMS and central count voting system platform, they will be required to install only software originating from the NYS

Certified Software Distribution as per guidance in the Voting System Software section of this policy.

EMS and central count voting system installation and use shall meet the following requirements:

- The EMS and central count voting system hardware cannot be used for anything other than voting purposes.
- EMS and central count voting systems shall remain in CBOE secure control at all times. If the EMS and central count voting system is determined to be out of CBOE secure control, the system hard drives shall be formatted and the EMS and central count voting system software installed from trusted media.
- All non-voting systems software not required for voting purposes shall be removed.
- Software not required for voting purposes cannot be installed on the EMS and central count voting system.
- The EMS and central count voting system cannot connect to anything other than a closed network.
- CBOEs shall seek approval of NYSBOE prior to installing any software that is not part of the NYS Certified Software Distribution.
- The facility or site in which the EMS and central count voting system is stored and used shall have controls in place to restrict physical access to authorized individuals. All access to the EMS and central count voting system shall be restricted to personnel who require physical access to perform their jobs. Access restrictions also apply to all voting equipment, computers, network equipment, and network cabling.
- If at any time an EMS and central count voting system is not maintained under CBOE secure control, the EMS and central count voting system shall be reinstalled from the NYS certified software distribution.

3.9 Closed Network

For purposes of this policy, a closed network is a Local Area Network (LAN) that is restricted (closed) in that it only connects an EMS server or servers, or central count voting system to specific workstations within a local environment, typically a room or building. All systems that connect to the closed network are dedicated solely to election configuration and ballot creation, vote result reporting, and associated uses. The closed network cannot be implemented via a virtual private network or in any way that results in the closed network being part of, or connected to, any other network. All servers and workstations that are part of the closed network are dedicated solely to election-related tasks described herein and may not be connected to any other network or used for any other purpose at any time. Closed networks shall be hardwired together using network cables and cannot have any kind of wireless or infrared functionality.

Voting systems certified or authorized for use in NYS are prohibited from being connected to any network other than a closed network. Precinct Based Optical Scanners (PBOSs), Ballot Marking Devices and Central Count Optical Scanner (CCOS) Systems may never be connected to any network.

3.9.1 Use of a Closed Network

County Boards of Elections are permitted to use a closed network to aid with the following election tasks:

- Creating ballot and election definitions
- Populating ballot and election definitions on removable memory devices that are then installed in voting systems to be used in an election
- Transferring election results from removable memory devices into the EMS
- Supporting the EMS for the collection and consolidation of PBOS and CCOS election results to aggregate results
- Supporting the counting of ballots on a central count voting system

3.9.2 Closed Network Topology

A closed network consists of one or more EMS servers and one or more dedicated EMS client workstations or a central count voting system that are connected via a network device. The closed network is configured to support only local subnets. The closed network cannot be connected to any other network.

3.9.3 Closed Network Usage Requirements

Closed networks are permitted to be used subject to the following restrictions:

- Closed networks are contained entirely within a secured facility, which shall have controls in place that restrict physical access to authorized individuals.
- All devices (EMS servers and workstations) connected to the closed network shall be protected via the use of passwords.
- Closed networks shall not be extended to any poll site location.

3.10 Voting System Logical Security Controls

3.10.1 Account Management

All accounts used to access voting systems in any way shall only be used by a single individual. Sharing of accounts and account credentials is prohibited. The ESSOs shall ensure that processes are in place for voting system account maintenance with designated persons responsible for the administration of accounts for the full life cycle of the account.

If a person changes roles (or job responsibilities) and no longer requires access to a voting system, that person's account shall be disabled or deleted as soon as possible after the access is no longer necessary.

3.10.2 Administrator Accounts

If persons with administrative accounts are assisting in the performance of election tasks not related to the administration of the voting system, they shall perform such work using their voting system user account and password, not their administrative account and password.

If necessary, a system administrator account may utilize a split password. In this case, account access is controlled by the need to have two individuals present where each individual knows half of the password. All use of the administrator account is therefore done with both party representatives present. The use of administrator level accounts shall be minimized, as should the use of a split password whenever possible.

3.10.3 Account Recertification

A periodic account-recertification procedure shall be in place to review every account and certify that the owner of the account still requires access to the system that the account provides. All accounts should be recertified whenever CBOE staff roles change or, at a minimum, yearly.

3.10.4 Password Management

Passwords of all accounts in the voting system shall be changed before testing and configuration of a new election begins.

If at any time the CBOE discovers that any password has been lost, shared, or otherwise compromised**,** all passwords shall be changed and the Security Incident Response Procedure shall be executed as needed.

4. TESTING OF VOTING SYSTEMS

The following is required for all testing of voting systems and is more fully detailed in part 6210 of Subtitle V of Title 9 of the Official Compilation of Codes, Rules and Regulations of the State of New York:

- All voting systems shall be tested before use in any election.
- CBOEs shall conduct quarterly maintenance testing of voting systems.
- Pre-Qualification testing shall always include the use of the approved software-validation methods as appropriate to the device being used in an election. Testing shall include the processing of specifically designed test decks while the system is in election mode —just as it would be during an actual election.
- Testing shall determine that the system is functioning correctly and that all system equipment, including but not limited to hardware, memory, and report printers, are properly integrated with the voting system and capable of properly performing in an election.
- Testing procedures shall be approved by NYSBOE.
- As per the security incident response procedure, software validation methods or software re-installs are also required whenever the integrity of the system is in question.
- Results from each test shall be recorded on a maintenance log that is associated with each voting system.
- All documentation and/or test decks, simulation cartridges, and any test data, including but not limited to copies of ballot programming used for required maintenance tests, shall be maintained in secure locked storage as per NYS Election Law and record retention requirements.
- Voting system maintenance logs are to be kept as a permanent record of the CBOE and entered into the asset management software.

5. VOTING SYSTEM MODE SECURITY REQUIREMENTS

5.1 NYSBOE Acceptance Testing

Acceptance testing of voting systems shall be conducted under the supervision of NYSBOE as per NYS Election Law and Subtitle V of Title 9 of the Official Compilation of Codes, Rules and Regulations of the State of New York.

Acceptance test means a test conducted by the county board under the supervision of the State Board, to demonstrate that each voting system delivered, when installed in the user's environment, meets all functional requirements and contains exactly the same components as the voting system of that type, which received certification from New York State, including but not limited to all hardware, programming (whether in the form of software, firmware, or any other kind), all files, all file system hierarchies, all operating system parts, all off-the-shelf hardware and programming parts and any other components.

5.1.1 County Receipt Process

The receiving CBOE shall conduct the acceptance test procedure under the supervision of State Board. Once delivery is accepted, the CBOE becomes responsible for protecting the voting system as per this policy.

Upon receipt of the voting system by the CBOE, the following is required:

- Each voting system received shall be inventoried to ensure that the shipment received matches that signed for by the driver.
- The voting system shall be logged into the CBOE inventory tracking system by the CBOE bipartisan team(s) assigned to this task.
- The CBOE shall update the NYSBOE asset management software as required.

  NOTE: If there is evidence of tampering, the security incident-response plan shall be invoked, and the State Board of Elections Operations Unit shall be notified immediately.

5.2 Storage Mode

When any voting system is not being tested, transported, used in an election, or undergoing a maintenance procedure, it shall be securely stored in a manner consistent with the Voting System Facility Guidelines for Storage, Power and Transportation Recommendations and Best Practices.

Whenever a voting system cannot be maintained in CBOE secure control, the Voting System Transportation Chain-of-Custody Procedure shall be followed.

The CBOE shall provide locked and secure storage with CBOE secure control for all voting systems, ballots, system test materials, copies of software and ballot

programming, programming devices, memory devices, disability access devices, voting system keys, key cards, and all ancillary devices of voting system components and materials.

5.2.1 Access to Systems during Storage Mode

During storage mode all voting systems shall be maintained in a secure, locked facility with all appropriate device locks and seals in place.

CBOEs must provide voting system storage that provides and maintains CBOE secure control at all times. When such control is provided, the use of tamper-evident seals and the Voting System Transportation Chain-of-Custody Procedure are not required.

Whenever CBOE secure control cannot be provided, the CBOE shall utilize tamper-evident seals and locks as per the Voting System Transportation Chain-of-Custody Procedure for all voting systems.

All access to the voting system storage facility and system components shall be restricted to personnel who require physical access to perform their job duties. Physical access controls should be implemented to prevent or log unauthorized access.

CBOEs shall adopt security procedures which restrict and document all access to voting systems. These controls shall enable CBOE secure control of voting systems.

Physical keys, cryptographic keys, passwords and security tokens for the voting systems shall be kept under CBOE secure control at all times, stored in a separate and secure location, and not stored with the voting systems themselves.

Whenever there is evidence or suspicion of unauthorized access to voting systems, the CBOE security incident response procedure shall be implemented.

5.3 Transportation Mode

5.3.1 Transportation Mode Defined

Transportation mode includes any and all times when any voting system is transferred during an election from one location to another and is not in CBOE secure control. Whenever voting systems are used and transported during an election the Voting System Transportation Chain-of-Custody Procedure shall be followed.

When voting systems are transported for non-election purposes, the voting system, upon return to the CBOE shall undergo the County Receipt Procedure and pre-qualification testing prior to the voting system being used in an election.

5.3.2 Vendor Servicing of Voting Systems

When voting systems must be transported to a vendor for service or repair, only the necessary components shall be sent and the Voting System Transportation Chain-of-Custody Procedure does not apply. Removable media should not be present when systems are transported to a vendor for service.

Whenever voting systems are returned from a vendor, the CBOE shall perform the County Receipt Procedure and pre-qualification testing prior to the voting system being used in an election.

5.3.3 Transportation of Election Result Data and Security Pack

Whenever election result data is generated or transported, the Election Result Data & Security Pack Chain-of-Custody Procedure shall be followed. Control and possession of the election result data shall be maintained at all times.

Whenever paper ballots are transported, the Voting Systems Transportation Chain-of-Custody Procedure shall be followed.

Security packets and secure ballot storage containers shall always be transported in full control and possession of CBOE staff or other designated individuals as per the Election Result Data & Security Pack Chain-of-Custody Procedure.

5.4 Installation and Maintenance Mode

Whenever a voting system is in this mode, it shall be kept in CBOE secure control. When CBOE secure control cannot be maintained, the Voting System Transportation Chain-of-Custody Procedure shall be followed.

If a voting system is outside of CBOE secure control and was not handled as per the Voting System Transportation Chain-of-Custody Procedure then the system shall undergo the County Receipt Procedure and pre-qualification testing shall be done prior to use in an election.

5.4.1 Pre-Qualification and Quarterly Testing

All voting systems shall undergo Quarterly and Pre-Qualification Testing. During this testing, all voting systems shall be protected as if they were in pre-election mode according to section 5.5 of this policy.

During any testing the protective counter values shall be documented at the beginning and end of testing.

5.4.2 Maintenance of Voting Systems

All vendor-prescribed maintenance tasks and diagnostic tests shall be conducted by the CBOE on all voting systems as required.

Whenever voting systems must undergo any type of maintenance or are removed from storage mode, they shall be protected as if they were in pre-election mode according to section 5.5 of this policy.

5.5 Pre-Election Mode

Pre-Election Mode is defined as the time when an election is prepared. This includes Pre-Qualification Testing of the equipment, defining elections, creating ballots, and configuring election devices with election and ballot data.

5.5.1 Pre-Election Mode Access to Systems

When being prepared for election use, all voting equipment, computers, network equipment, and network cabling shall be maintained in a secure, locked facility and shall be under CBOE secure control at all times. All access shall be restricted to personnel who require physical access to perform their pre-election job duties.

When voting systems are not being used for pre-election activities, they should be kept in CBOE secure control. If CBOE secure control cannot be achieved, voting systems shall be secured as per the Voting Systems Transportation Chain-of-Custody Procedures whenever they not in the control and possession of authorized CBOE staff.

All passwords of all accounts in the voting system shall be changed before configuration of the election and pre-qualification testing begins. Additionally, the purpose and need for each account shall be verified and should align with the roles of each CBOE staff member.

> **NOTE:** If there is evidence of tampering, the security incident-response plan shall be invoked, and the State Board of Elections Operations unit shall be notified as soon as practicable.

5.5.2 Audit Logs

The audit records from the election configuration, ballot configuration, and pre-qualification testing shall be prepared and maintained for a period as required by NYSBOE.

5.5.3 System Backup and Recovery

A system backup and recovery procedure, based on vendor and NYSBOE recommendations, shall be created and tested. The procedure will ensure that replacement election equipment can be obtained and/or used to configure the election should any election device or equipment have a catastrophic failure or be otherwise unavailable.

To ensure backup and recovery, master copies of all election configurations, ballot configurations, and all system software shall be maintained in secure, locked storage separate from the location of working copies.

The CBOE shall ensure that current backups of the voting system EMS, central count voting system, ballot definitions, templates and copies of all NYS certified software distributions and files necessary to conduct operations are also stored in a secure offsite storage facility.

The CBOE should periodically test their backup and recovery procedures to ensure they are working properly. Backup and recovery procedures should be tested whenever there is a software or hardware change to the EMS and central count voting system.

5.6 Election Mode

Election Mode begins when the voting system and all components are present at the poll site and the system is enabled for use during the election. This period ends when the polls are closed and the systems are secured against further voting.

5.6.1 Voting System Delivery and Storage at Poll Sites

Voting systems shall be transported to poll site locations as per the Voting Systems Transportation Chain-of-Custody Procedure. Whenever possible, each voting system upon delivery should be placed in a secure location with restricted access at the poll site until the poll workers arrive to set up the systems and prepare for the opening of the polls.

All physical keys and authentication tokens, as well as the security seal report forms, shall be maintained as per the Election Result Data & Security Pack Chain-of-Custody Procedure requirements and delivered in the security pack separately from the devices for which they are used.

Whenever possible, an authorized representative at the polling site shall sign the Transportation Manifest Form as presented by the CBOE's authorized transportation representative. This form shall be sent back to the CBOE upon completion of delivery so it can become part of the audit log for the device. Whenever possible, verification of all seals and locks shall be completed as per the Voting System Transportation Chain-of-Custody Procedure.

5.6.2 Tampering During Election Mode

If at any time there is evidence or suspicion of a security breach, the security incident response procedure shall be invoked, use of the voting system in question shall be halted, and emergency ballots or other methods of voting as per the security incident response plan shall be utilized.

5.6.3 Polling Place Security

Each CBOE shall have procedures on how to secure poll sites and equipment from the time the voting equipment is delivered until the equipment leaves the site. Each CBOE shall ensure that poll sites follow the Election Day poll site procedures.

5.6.3.1 Floor plans

The precinct-based voting equipment, voter check-in station, privacy booths, tables, and chairs shall be laid out in a manner that:

- Ensures that no unauthorized person can access a PBOS or BMD

- Ensures that voters who wish to obtain a new ballot (whether they have attempted to scan the ballot or not) may do so without having others know why they desire a new ballot
- Ensures that an affidavit voter is not permitted to scan their ballot for tabulation
- Ensures that no one can leave the poll site with a ballot
- Ensures that privacy booths are setup as per vendor and NYSBOE recommendations to ensure voter privacy

5.6.4 Privacy Booth Layout

Privacy booths, BMD equipment, and PBOS equipment shall be set up so that no poll workers or other voters can see the ballot a voter is preparing or casting. The screens of BMD and PBOS devices shall be arranged so that no one can view any of the messages that may be presented to a voter when a ballot is being cast or created on the device. Privacy booths that accommodate voters with disabilities shall be clearly labeled and configured to allow for a sufficient and clear path of travel.

Additional information can be found in the Election Day poll site procedures listed in Appendix B.

5.6.5 Election Day Ballots

- All ballots shall be accounted for.
- Ballots waiting to be distributed to voters shall be protected from theft or tampering.
- All spoiled ballots shall be clearly marked and stored in a secure ballot storage container, and shall be handled without comment, ensuring privacy.
- Once a ballot has been given to a voter, that ballot shall either be marked and cast by the voter or returned to inspectors to be spoiled.
- Ballots that have been voted shall remain in the ballot box until they are removed following the CBOE's approved procedures prompted by the close of polls, or the need to be transferred to a sealed secure container in order to prevent overflow issues has been determined by poll workers (PIT team).
- Provisions of the Election Day Poll Site procedures shall be followed to ensure adequate responses to any situation where the ballot box shall be opened before the close of polls. The confidentiality and integrity of the ballots, from the time they are removed from the voting device or ballot box until they are archived, shall be preserved. These procedures shall contain specific security instructions for poll workers when handling ballots to ensure that there is no possibility of accusation or suspicion of tampering with the ballots.

5.6.6 Poll Worker Procedures and Responsibilities

All CBOE staff and poll workers shall understand the security controls in place on the devices and the proper procedures for handling, securing, and using the devices and ballots to be cast or created on those devices.

All poll workers shall be aware of any attempts by anyone to access the devices outside of regular operating procedures and shall stop any such activity. Poll workers shall follow CBOE procedures for contacting a CBOE official if there are any questions or problems related to security procedures or equipment or to report a possible security-breaching incident.

CBOE staff and poll workers shall understand that all errors and voting system malfunctions shall be investigated, and the security incident response procedure shall be followed.

Poll workers shall inspect all devices regularly throughout Election Day to ensure that all locks and seals remain in place and that there is no sign of tampering.

> **NOTE:** If there is evidence of tampering, the incident-response plan shall be invoked, the CBOE shall be notified immediately, and the CBOE shall notify NYSBOE as soon as practicable.

5.6.7 Voting System Failures

In the event of any voting system failure, poll workers shall follow the emergency process steps documented in the relevant Election Day Poll Site Procedure, and ensure that the failed system cannot be accessed by voters, and shall affix a sign to the scanner's 'INSERT BALLOT HERE' component, to that effect. Voting can and should continue when any voting system has failed. Voters shall continue to mark their ballots, and shall place marked ballots into the emergency ballot box component of their respective scanner, or into a separate; secure emergency ballot box container which shall be appropriately labeled, until such time as a replacement scanner, if one is available, is delivered or until the close of polls.

If the voting system failure is an extended one, and the device's emergency ballot box becomes filled with voted ballots, such ballots may be removed on a periodic basis. These ballots may be deposited into an alternate, portable and secure emergency ballot box, bag or other secure package or secure ballot storage container, as provided by the county board of elections, which is clearly labeled FOR EMERGENCY BALLOTS ONLY.

County boards of elections may choose to purchase a quantity of emergency ballot boxes or other secure ballot storage containers which can be used for this purpose. Depending upon the type of secure ballot box or storage bag the county board may choose to purchase, this item may be delivered with Election Day supplies, or they may be delivered on an as-needed basis by board of elections staff, upon notification that emergency ballots are being cast and the scanner outage may be an extended one.

For small scale, large scale, or poll site-wide failures, the county board's contingency plan shall be followed.

5.7 Post-Election Mode

All procedures created for closing polls, printing results, and removing media from election systems shall contain specific security steps and requirements to assure no possibility of accusation or suspicion of poll workers tampering with equipment, ballots, or results. All poll workers shall be trained in these procedures.

Immediately before canvassing or printing of reports, all tamper-evident security seals shall be verified to be in place, not to have been altered, and the seal numbers verified and recorded in the Transportation Manifest Form as per the Voting System Transportation Chain-of-Custody Procedure.

> **NOTE:** If there is evidence of tampering, the incident-response plan shall be invoked, the CBOE shall be notified immediately, and the State Board of Elections Operations Unit shall be notified as soon as practicable.

5.7.1 Election Result Data Chain-of-Custody

All Election Result Data shall be maintained as per the Election Result Data & Security Pack Chain-of-Custody Procedure.

Authorized poll workers at the poll site shall maintain the election result data & security pack chain-of-custody forms for all election result data and each voting system.

5.7.2 Canvass of Votes

Each CBOE shall ensure that the canvass of votes is completed as per the Election Day Poll Site Procedures. During the canvass of votes, the Election Result Data & Security Practice Chain-of-Custody procedure shall be followed.

5.8 System Disposition

Whenever any voting system or component is disposed of or otherwise retired from service, the CBOE shall ensure that all voting data, software, and firmware has been removed or cleared. NYSBOE-approved memory cleansing software or hardware shall be used to ensure that all data is removed. CBOE system disposal procedures shall be created and approved by NYSBOE. System disposition is to be logged in the asset management software.

5.9 Compliance

Compliance with this policy is mandatory for CBOEs to help ensure that elections are conducted in a consistent and secure manner across NYS. CBOE Election Commissioners and the CBOE ESSOs are responsible for certifying to NYSBOE that the policy has been complied with.

5.10 NYSBOE Monitoring

As part of its mandate to oversee elections operations throughout the state, the NYSBOE Operations Unit will incorporate into its CBOE visits a physical audit of CBOE assets and a review of CBOE storage sites, workspaces, chain-of-custody logs, asset management logs, and other aspects of voting system ownership, deployment, and use to evaluate overall compliance with this and other related policies. NYSBOE will provide reports to the CBOE so that, if and where necessary, steps for remediation can be taken.

6. DEFINITION OF TERMINOLOGY

6.1 Reference Abbreviations Used in Definitions:

New York State Election Law

6209- Part 6209 of Subtitle V of Title 9 of the Official Compilation of Codes, Rules and Regulations of the State of New York

6210- Part 6210 of Subtitle V of Title 9 of the Official Compilation of Codes, Rules and Regulations of the State of New York

VVSG Vol 1- Election Assistance Commission's 2005 Voluntary Voting System Guidelines

6.2 **Definitions** (origins referenced where applicable)

acceptance testing: (from 6209) A test conducted by the county board and the state board, to demonstrate that each voting system delivered, when installed in the user's environment, meets all functional requirements and contains exactly the same components as the voting system of that type which received certification from New York State, including but not limited to all hardware, programming (whether in the form of software, firmware, or any other kind), all files, all file system hierarchies, all operating system parts, all off-the-shelf hardware and programming parts, and any other components.

access control(s): Technologies and procedures designed to limit access to a system or data to only those who are approved.

accountability: Property that ensures there is an ability to determine when actions or events occurred in a voting system and which specific individual or component executed them.

anti-virus: Software on a device that attempts to detect and stop malicious and unwanted programs (that is, programs that may harm the system) from being installed or run on the system.

asset management software: NYSBOE software program to track all voting system components as per federal, and state guidelines.

audit: (From VVSG Vol 1) Systematic, independent, documented process for obtaining records, statements of fact, or other relevant information and assessing them objectively to determine the extent to which specified requirements are fulfilled.

audit data: (From VVSG Vol 1) Recorded information that allows election officials to review the activities that occurred on the voting equipment to verify or reconstruct the steps followed without compromising the ballot or voter secrecy. This can be events about a device (e.g., software/firmware upgrades) or about an election (e.g., Election created, contest defined, vote cast, ballot marked), and can come from the audit log of the election software and the Operating System (OS) logs of the device.

audit log: See audit data.

audit trail: See audit data.

availability: (From VVSG Vol 1) The percentage of time during which a system is operating properly and available for use.

ballot: (From VVSG Vol 1) The official presentation of all of the contests to be decided in a particular election. (From New York State Election Law) The word "ballot," when referring to voting machines or systems, means that portion of the cardboard, or paper, or other material, or electronic display within the ballot frame containing the name of the candidate and the emblem of the party organization by which he or she was nominated, or the form of submission of a proposed constitutional amendment, proposition referendum or question, with the word "yes" for voting for any question or the word "no" for voting against any question.

ballot definition: (From VVSG Vol 1) Information that describes to voting equipment the content and appearance of the ballots to be used in an election.

ballot marking device (BMD): A device that only provides the capability to mark a paper ballot and has no recording or tallying capabilities.

ballot image: Digital representation (picture) of a scanned ballot that can be viewed for audit or other post-election purposes.

ballot records: Electronic interpretation of how the scanned ballot marks were recorded and associated with each contest or proposition.

breach: A voting system, election data, or election process whose availability, confidentiality, accountability, or integrity has been or appears to have been compromised.

CBOE staff: The county board of elections staff that is responsible in some manner for the preparation and execution of an election. This includes county board employees and contractors, as well as poll workers, coordinators, voting system technicians/custodians, etc.

CBOE secure control: This defines a state of control of voting systems, components, or election result data when they are under the possession and control of the CBOE or CBOE staff. Possession and control means that only authorized individuals are permitted access to the voting systems, election day ballots and election results, authorized access is logged and unauthorized access is detectable, voting system locks are used, and keys are not stored with the voting systems.

central count optical scanner system (sometimes referred to as "Central Scanner", "Central Count Optical Scanner" or "Central Count Voting System"): A voting system that uses optical scan technology to record and tabulate votes from multiple election districts at a county board office, including all absentee, emergency, affidavit, and other such paper ballots. A central count optical scanner system and any other components (i.e. EMS, server(s)) necessary for use and connected by a closed network.

certified voting system: A voting system that has been tested and approved for use in New York State by the NYS Board of Elections.

Chain-of-custody form: (See transportation manifest and seal tag reports)

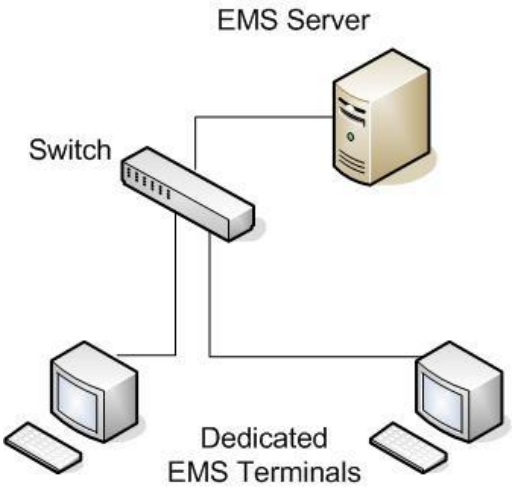
Chain-of-custody log: A log which tracks every time a voting device has been moved and which contains the collection of all completed chain of custody forms for the unit.

change management: Process of approving, testing, and implementing changes to a system in a controlled manner to limit problems that may arise and to ensure that the system's configuration stays properly documented.

client workstations: Computers which are dedicated solely for elections work and used by election workers on a closed network for EMS systems that have a client/server model.

close poll: The act of closing the poll and ensuring that voting has ceased.

closed network: A closed network is a stand-alone Local Area Network (LAN) that is restricted (closed) in that it only connects an EMS server or servers, or central count voting system to specific workstations within a CBOE local and controlled environment, typically a room or building. The closed network is restricted to specific workstations and users and not connected to any other internal or external network. A standalone EMS system that is self-contained can also be considered a closed network. The diagram below depicts the Closed Network topology for an EMS server but would also apply for a central count voting system.



component or device: A single unit or subset of a voting system. For example, EMS server and/or workstation, Scanner, BMD, or the Removable Media used to transfer data between each component.

confidentiality: Property that ensures election information, data, and voting systems are only accessed by individuals authorized to access the information.

configuration management: Process of identifying and maintaining configuration information for voting systems, recording and reporting the status of the voting systems' configuration information and requests for change, and verifying the completeness and correctness of voting systems.

contingency plan: A plan describing how an election will be carried out in the event of an unanticipated or unavoidable event. The plan will seek to minimize potential losses or failures and facilitate recovery of the election process in a timely fashion.

COTS: (From VVSG Vol 1.1) Software, firmware, device or component that is used in the United States by many different people or organizations for many different applications other than certified voting systems and that is incorporated into the voting system with no manufacturer- or application-specific modification

cryptographic key: (From VVSG Vol 1) Value used to control cryptographic operations such as decryption, encryption, signature generation, or signature verification.

cryptography: (From VVSG Vol 1) Discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, prevent their undetected modification, and establish their authenticity.

decryption: (From VVSG Vol 1) Process of changing encrypted text into plain text.

device management data: This is configuration and management data about voting devices used by the system (BMDs, Scanners, etc). This data can be stored on the device itself, in the EMS, or on mobile media.

digital signature: (From VVSG Vol 1) An asymmetric key operation where the private key is used to digitally sign an electronic document, and the public key is used to verify the signature. Digital signatures provide data accountability and integrity protection.

disaster recovery: Plans and procedures that are in place to quickly recover from the unexpected loss of any resource(s) necessary for the completion of a process or task.

election configuration data: Districts, parties, candidates, propositions, contests, ballot formats, election layout, configuration information, and other data needed to configure a voting system to conduct a specific election.

election information: All the data, information, reports, and physical objects (inputs and outputs) created as a result of an election. This includes election configuration data, ballot images, paper ballots, ballot records, election-result data, generated reports, and audit information.

election management system (EMS): The system that provides functions and databases within a voting system that is used to define, develop, and maintain election databases, performs election definitions and setup functions, formats ballots, counts votes, consolidates and reports results, and maintains audit trails. In NYS, the EMS is permitted to be either a standalone system or connected to a closed network.

election mode: This period begins when the voting system and all components are present at the voting site and the system is enabled for use during the election. This period ends when the polls are closed and the system is not able to be used in the voting process. (From 6210), An operational setting and/or functional level of a voting system that would allow the user, under the required conditions stated by law, to make selections and/or cast a ballot, and which also uniquely provides the potential to have a marked ballot officially accepted for counting at the time of a defined election. Note: This mode of operation may also be synonymous with the term "live vote mode" or similar. This mode may also be run at any time, either for the running of pre-election or pre-qualification and/or after various maintenance activities. This mode is specifically required to be run in the conduct of an official election. Election Mode can also be used in contrast to Test Mode.

election result data: All data, electronic or paper, that is generated during an election that could be used to determine the outcome of an election. This includes all voted paper ballots, election reports, audit data, ballot images, and ballot records. The total of votes cast for each contest or proposal on a voting device or across voting devices (precinct totals, etc).

election result data & security pack chain-of-custody: The process and associated documentation that provides the chronological documentation showing the possession and transfer of all election result data or security pack.

election software: Any software or firmware, including operating-system software, commercial-of-the-shelf (COTS) software (e.g., Database Management Systems), and voting system vendor-supplied software, that can directly or indirectly influence the outcome of an election. Election software represents all software that shall be trusted, protected, and validated accordingly.

election software and firmware reference information (hashes): This is the "fingerprint" or cryptographic hash value of all the election software or firmware installed on all voting system devices. When the Software Validation check is done, this reference data is compared to the hash data retrieved from the device to ensure that the software on the device has not been altered from the current, certified version.

election systems security officer (ESSO): Role assigned to bi-partisan county staff to be responsible for the development and adoption of security procedures and the implementation and monitoring of information-security policy.

election worker: CBOE staff assigned to work at a poll site or sites.

encryption: (From VVSG Vol 1) Process of obscuring information by changing plain text into cipher text (unreadable text) for the purpose of security or privacy.

firmware: Computer software that is stored in non-volatile memory .

hash function: (From VVSG Vol 1) A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties: 1.) (One-way) it is computationally infeasible to find any input that maps to any pre-

specified output, and 2.) (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output. The output of the Hash Function is the hash of the data.

installation and maintenance mode: This is use of the system when outside of the Pre-Election, Election, Post-Election, Storage, and Transportation modes. This would include, for example, software installation, software updates, court-ordered audits, quarterly maintenance testing, etc.

integrity: Property that ensures election information, data, and voting systems do not change, except through defined processes and by approved/authorized personnel.

internal audit log: (From VVSG Vol 1) A human readable record resident on the voting machine, used to track all activities of that machine. This log records every activity performed on or by the machine, indicating the event and when it happened.

logical access: The collection of policies, procedures, and electronic Access Controls that permit controlled access to a voting system.

maintenance log: (From New York State Election Law) A written and/or electronic record which contains all information relating to performance of scheduled and nonscheduled maintenance on a voting system, all service visits performed by the vendor or manufacturer, and other maintenance or service performed by any other provider of service, including county and state board employees.

mode of use: The various modes (states) in which a component can exist. Valid modes include: Storage, Pre-Election, Election, Post-Election, Transportation, and Installation and Maintenance.

NYS certified software distribution: Read-only media containing all installation files and software necessary to install all voting system software on a NYSBOE certified voting system component.

operating system: The low-level software on a hardware device that allows programs to run and users to interface with the device.

paper-based voting systems: (From 6209) Any electronic or computerized ballot-counting system or equipment that tabulates and reports votes cast on paper ballots.

password: 1) A group of characters (letters, numbers, and/or special characters) that is known only to the user to authenticate the identity of the user. 2) A group of characters (letters, numbers, and/or special characters) that shall be entered by the user that controls access to a system, system function, or functions.

patch: Periodic updates from a software or system vendor to fix bugs or add functionality to the software or system.

physical access: Having access to a facility, resource, system, or physical media. For the purpose of this policy, the term is used to describe having physical access to the voting system itself.

post-election mode: This period begins after the polls have closed and tabulation begins at the poll site. This mode continues at the CBOE, where additional canvassing is done and election results are gathered and archived.

precinct based optical scanner (PBOS, sometimes referred to as **"scanner"** or **"tabulator"):** (From New York State Election Law) A voting system at the polling place in which a voter records his or her vote by placing a mark in a designated voting response field on a paper ballot or card, which is read and tabulated using optical-scan technology or a mark-sense system that reads the paper ballot or card by scanning the ballot and interpreting the contents. Ballots may have been marked either by hand or by a Ballot Marking Device (BMD). These systems typically tabulate ballots as they are cast and print the results after the polls have been closed. PBOS systems store election results and other election-related data on electronic media.

pre-election mode: This begins when voting systems are removed from storage where preparations begin for use during an election. This period includes the programming and configuration of voting systems for use in an election within an environment controlled by the CBOE.

pre-qualification test: (From 6210) A test prescribed by the State Board, conducted immediately prior to the voting system's use in an election in which a predetermined set of votes are cast, which will ensure that all voting positions for each ballot configuration are tested. Such votes shall be entered into the voting system in the same manner in which they are entered by voters during an election. If a voting system offers several methods for votes to be entered, such as touch-screen, push-button, or other electronic mechanism, a key pad and/or pneumatic switch for voters with disabilities, or alternate language displays, then a predetermined set of votes shall be entered separately using each method and language display. The results of the casting of said votes and all voting system logs shall be extracted from the system as though during normal use in an election, and the results and logs shall be compared to the predetermined results of the test votes and vote totals prepared pursuant to regulations and procedures of the State Board.

private key: (From VVSG Vol 1) The secret part of an asymmetric key-pair that is typically used to digitally sign or decrypt data.

privacy booth: A compartment in which the voter marks their ballot, which provides physical protections from others viewing how the voter is voting the ballot.

privacy sleeve: A device that is used to protect the confidentiality of paper ballots within the poll site. After voting a ballot, the voter uses this sleeve to protect the secrecy of their vote throughout the remainder of the voting process at the poll site.

protective counter: (From 6209) For a voting device, this records the number of times the machine or system has been operated since it was built.

public counter: (From 6209) For a voting device, this records the number of persons who have voted on the machine at each separate election.

public keys: (From VVSG Vol 1) Public part of an asymmetric key-pair that is typically used to verify digital signatures or encrypt data.

quarterly maintenance testing: Tests of voting systems conducted by the CBOE during pre-defined periods during the year as per Part 6210 of Subtitle V of Title 9 of the Official Compilation of Codes, Rules and Regulations of the State of New York. These tests include software verification an calibration testing via the use of a test deck.

removable media: Electronic media containing election configuration information, election results, and audit logs that can be removed from a voting system.

result printout (results tape): These are printed reports produced by the PBOS and used to tally results or show system status and are kept for audit purposes. Printout means either the printed copy of zero totals; candidate names, offices, and other information produced by the voting equipment prior to the official opening of the polls; or the printed tabulation report of votes cast at the close of the polls.

secure ballot storage container: A secure storage container specifically for paper ballots.

secure cryptographic hash: A cryptographic hash implementation that has been validated by NIST and listed in FIPS 180-3.

security incident: A breach or the appearance of or potential for a breach.

security incident reporting log: Log used to record the fact that a CBOE Security Incident Reporting Form was filled out to report a suspected or actual security incident.

security incident response: Defined process and procedures to discover, investigate, and resolve breaches and adverse events or situations that could cause harm or potential harm in an election system.

security incident response team (SIRT): A team of individuals who are qualified to investigate all security incidents. CBOE SIRTs can be comprised of in-house staff or contracted as needed.

security incident reporting form: Form used to record information about a suspected security incident when it is first reported. The form identifies the incident and records a summary of the actions taken.

security investigations: A component of the incident response program that provides for the investigation of security breaches and incidents whenever they involve a CBOE voting system or election process.

security pack: A pouch, portfolio, or similar container that has a means of being sealed, which provides election inspectors with a single and secure source for storing seals, tags, chain-of-custody form, keys, and other security-related documents, as well as the removable memory device containing results, etc. Note that a secure ballot storage container can also be used as the security pack.

security procedure(s) Detailed CBOE and vendor specific operating procedures that are necessary to implement this policy.

Security seal/tag reports (forms): This document is a system-specific chain-of-custody form that serves to record all security seals and tags placed on each unit at the CBOE in preparation for use on Election Day and provides spaces for election inspectors to confirm seals as intact and unaltered at the opening of polls. Additionally, the manifest has spaces where inspectors can log security seals that need to be used during Election Day, as well as those that need to be used at the close of polls.

secure storage container: Any container that has locks and/or tamper-evident seals and is built to withstand opening or tampering with contents, except by using keys for the locks, or the breaking of tamper-evident seals consistent with corresponding procedures. A PBOS can be used as a secure storage container.

security token: A physical device that is used to authenticate a user. Examples include iButtons and one time password generator devices.

software validation: A process to ensure that all software on a device has not been changed and that no new or additional software has been added. (Sometimes referred to as "Hash Check" because of the methodology of the software-validation process.)

software validation information: The information (HASH values) used to validate the integrity of software as part of the Software Validation process.

software validation tools: NYSBOE-certified software and hardware (in some cases) provided by the vendor or NYSBOE that are used to extract and validate software and firmware from voting systems against software validation information.

spoiled ballot: Ballot that has been returned by the voter in exchange for a replacement ballot.

storage mode: Storage of voting systems and election information when not in use during an election and when not being transported or maintained.

system hardening: Configuration **s**teps applied to a system to ensure that the system is resilient to attack or compromise.

system administration procedures: CBOE-specific procedures for how to administer and maintain the voting systems. These procedures will address how software and configuration management will be done.

tabulator: See "Precinct Based Optical Scanner System."

tamper-evident security seal: Devices such as tape, locks, straps, or bands that are used to indicate that access to a door or enclosure has occurred. The seal does not necessarily prevent opening the door or enclosure, but rather will indicate that access has occurred or was attempted.

test deck: (From 6209) A pre-audited group of ballots prepared for each election. The ballots are voted with a pre-determined number of valid votes for each candidate, each

write-in position, and each voting option on every proposal that appears on the ballot as certified by the county board. The deck includes one or more ballots that have been improperly voted, or which are voted in excess of the number allowed by law, and one or more ballots on which no votes are cast, in order to test the ability of the system to recognize and/or notify of an under or over vote. It also includes one or more ballots on which two or more votes are cast for a candidate whose name appears on the ballot more than once for the same office, in order to test the ability of the system to count only the first of such vote for the candidate. If there is more than one ballot style for an election, a separate test deck is created for each ballot style.

test mode: (From 6209) An operational setting and/or functional level of a voting system that would allow the user to specify/select, access and/or test various levels/areas of the device either, for example, during possible upgrades, diagnostic testing and/or specific maintenance activities that may not require full functional simulation or capabilities at that time. Note: This mode of operation is a separate option from Election Mode and is prohibited from being run in the conduct of an official election.

token(s): see Security Token

transportation manifest (form): Voting system transportation manifest form serves to track the round trip travel of each voting system from pick-up at the CBOE storage facility to poll sites or off-site vendor service site(s). This form shall be used whenever voting systems are transported between different locations. The voting system transportation manifest form will also contain tamper-evident security seal reference information.

transportation mode: This period defines the time when a voting system and election information is transferred between locations.

voted paper ballot: Paper ballots that have been marked by a voter and cast.

voting system(s): (From New York State Election Law) The total combination of mechanical, electro-mechanical, or electronic equipment and any ancillary equipment and all software, firmware, and documentation required to program, control, and support the equipment, all of which is used to define ballots, cast and count votes, report and/or display election results, and maintain and produce any audit trail information. This includes all PBOS, CCOS, BMD and EMS systems, including all client and server systems. The voting system also includes all electronic components that comprise the closed network.

voting system software: (From VVSG Vol 1) All the executable code (software or firmware) and associated configuration files needed for the proper operation of the voting system. This includes third-party software such as operating system, drivers, and database management tools.

voting system transportation chain-of-custody procedure: This procedure outlines the requirements that are in place whenever a voting system is transported from one

location to another. It identifies the steps to be taken to properly transport a voting system and prescribes proper use of the voting system transportation manifest form document.

7. APPENDIX A: REFERENCES

The following documents were utilized in the development of this policy:

- State of New York Election Law
- Subtitle V of Title 9 of the Official Compilation of Codes, Rules and Regulations of the State of New York, Parts 6209 and 6210
- Election Assistance Commission's 2005 Voluntary Voting System Guidelines (VVSG) Volumes I and II
- NYS Office of Cyber Security and Critical Infrastructure Coordination Cyber Security Policy P03-002

The findings resulting from research into voting system best practices across other states were also considered in the drafting of this policy, as was feedback from the 2009 Pilot Implementation Project and the New York State Election Commissioners' Association Pilot Review Committee as well as from continued use of these systems.

8. APPENDIX B: TABLE OF APPLICABLE SECURITY PROCEDURES AND TEMPLATES

Template versions of mandatory procedures listed below can be found at - https://nysemail.sharepoint.com/sites/CBOE/_layouts/15/start.aspx#/SitePages/Home.aspx.

Plan and Procedures and Templates	*Purpose*
Pre-Qualification Test Procedure	Defines steps necessary to conduct pre-qualification testing
Quarterly Maintenance Test Procedure	Defines steps necessary to conduct Quarterly testing
Test Deck Procedure	Defines steps necessary to prepare ballots used for testing purposes
Acceptance Testing Procedure	Defines steps necessary to perform voting system acceptance testing.
County Receipt Procedure	Defines steps necessary to perform during the initial county receipt of the voting systems.
Election Day Poll Site Procedure	Defines all required security procedures for voting system election mode use necessary to comply with the security policy and steps necessary to perform post-election activities
24-Month Archiving Procedure	Defines steps necessary to archive election results upon completion of an election.
Hash Check Procedure	Defines steps necessary to perform software validation testing
Voting System Security Seal Procedure	Documents how to properly prepare a voting system for use or transport with tamper evident security seals.
Election Result Data & Security Pack Chain of Custody Procedure	Procedure that documents the required chain-of-custody steps to follow when election result data or security packs are handled.
Voting System Transportation Chain of Custody Procedure	Procedure that documents the required chain-of-custody steps to follow when

	voting systems are handled.
Voting System Facility Guidelines for Storage, Power and Transportation Recommendations and Best Practices	Defines steps necessary to complete test deck testing
County Board of Election Operational Contingency Plan/Template	Defines the roles and processes that are followed when election processes are disrupted by outside or unavoidable events.
Change Management Procedure	Defines the procedure for managing change
Security Incident Response	Defines the roles and processes for dealing with a security incident.
EMS System Installation & Hardening Procedure	Contains procedures for secure installation and hardening of voting systems
Logical Security Controls Procedure	Defines the procedures to ensure that logical security controls are implemented properly.
System Backup and Recovery	Defines steps necessary to comply to provide for the backup and recovery of voting systems.
System Disposition	Voting system end of life procedures