

Voting System Security Policy

Security of any Direct Record Electronic or Optical Scan computer based voting system should provide:

-audit data that is sufficient to track the sequence of events that occur on the system and, to the extent possible, identify the person(s) that initiated the events

-must be well defined and strictly enforced policies and procedures that control who can access the system, the circumstances under which they can access the system, and the functions that they are allowed to perform on the system.

-there must be physical security in place such as doors and locks that control and limit access to the equipment.

1. Access to the System:

- Only operating system and voting software loaded
- Controlled access with authorized users

The computer-based voting system should have the full participation of your county IT Security procedures. The computer should have only the operating system and voting software loaded. Additional applications could jeopardize system security.

If the computer has no outside connections, it can only be accessed by county election staff or other authorized persons. Any such system should also have password requirements. There should be strict procedures that control who has access to the election system, when they can access the system, what components they can access, and what functions they are allowed to perform.

The computer portion of the election system should contain features that facilitate overall security of the election system. Primary among these features is a comprehensive set of audit data. For transactions that occur on the system, a record is made of the nature of the transaction, the time of the transaction, and the person that initiated the transaction. This record is written to an audit log to allow the sequence of events surrounding the incident to be reconstructed.

A security program, similar to a virus detection program, should be run against the operating system and the election tabulation software before beginning the definition of an election to verify that the code has not been altered. This program could be repeated after the close of the election to verify that the code did not change during the election.

Permanent storage of media containing certified application programs should be within a secure, fireproof location such as a safe. Additional backup copies of application programs and media containing election data should be created and stored securely off site.

Software/Hardware Highlights

- System reliability is a mandatory requirement
The Service Provider shall clearly state its approach to system recovery time loss and resultant degradation of processing capability. Support for full replication of voter database, signature and source document images shall be provided.
- Provide security within the application and the network operating system
Ensures that access rights and privileges are controlled and secure through the application and operating system.
- Provide a disaster recovery plan
Must provide the capability to restore data and recovery processing election management operations in the event of a disaster.
- Transaction auditing function
The Service Provider shall deliver a product that with the ability of their software can track a minimum of at least the name of the operator who makes any addition or change to any record or table in the voter registration database, the date and time of the change, and the value of the data element in the record before and after the change.
- Database security management capability
The management capability allows up to two (2) persons to act as security and recovery managers, controlling access and authorization privileges for all other users. Provides system administrators with the capability to track and limit access by functional need. This security measure in the system must also provide solutions that permit access to the system's application files from remote sites, such as during early voting, while maintaining appropriate levels of data and system security.
- Levels of access and authorization privileges
The system shall provide a document and reliable capability by which the security managers can grant different levels of access and authorization privileges to separate modules in the integrated database application.
- Capability to recover corrupted or destroyed files
The system shall provide solutions that enable the successful recovery of damaged, destroyed or corrupted files.
- Support the full replication of voter database, signature and affidavit imaging
The system shall support these functions by means of hard drive mirroring.

- Application password creation
The software solution shall allow the system administrator(s) to establish individual user passwords for access to the application, apart from passwords required for network and operating system access.
- Password maintenance
The System Administrator(s) shall be allowed to establish a “password life” so users must change their passwords periodically.

2. Testing Voting Equipment:

- Public test prior to election
- Test before public test
- Print zero totals
- End of day totals

Voting equipment should be tested when it is first received from the vendor. Tests should cover all functions that will be necessary to conduct an election. Prior to use in an election, each voting machine should undergo system diagnostics to ensure proper operation of certified components. A checklist confirms the outcome of acceptability. Any component failure should be logged and repairs to equipment performed as soon as practical.

3. Polling Place Security:

- Hardware security
- Software security
- Poll worker procedures

The county board of elections office should, to the extent possible, designate polling sites that afford the necessary security features and should maximize the use of whatever security features exist.

The memory cartridge for each voting panel should be stored within a secured compartment. The Chief Judge and Judges or service technician should be the only persons with access to this compartment. The memory cartridge and/or ballots from each voting location are transported from the voting location to the county elections office by a Judge.

The area of the voting enclosure that contains the voting machines must remain secure. A voter is not allowed to enter this area until a voting panel is available for his or her use. No person other than a voter, a person assisting a voter, a poll worker, or a machine technician may enter this area.

Voting machine protective counters should be observed and recorded with a date of record periodically throughout election day. Voting machines and ballot boxes should be sealed before delivery to polling place locations. Seals should be serialized with numbers. Logging

of machine serial number, seal number and designated voting location is an essential part of the audit trail.

Equipment Delivery: Voting equipment delivery to polling place locations should be conducted with the same degree of control as applied to storage. A delivery person or company should continue the audit trail for the election officials. Documentation and daily reporting are essential.

- The delivery person or company should provide documentation containing voting machine numbers for each voting location where equipment has been delivered.
- County Board of Elections staff should be assigned to supervise and document the proper delivery of the voting equipment.
- A list of persons involved in equipment delivery should be maintained by the county election office.
- Voting machines should remain stored in a secure location at the polling place. Additional supplies delivered with machines should be secured with the voting equipment.
- Polling places should be in locked buildings or locations that are capable of monitoring secure storage of voting equipment.

Election Worker Security Awareness and Requirements: All election judges are responsible for maintaining the security of the polling place, the integrity of the vote and the protection of voting equipment and supplies. Judges must be vigilant throughout election day and be aware of who is in the polling room. Frequent monitoring of voting machines and securing voting supplies ensures that any malicious attempt to compromise the accurate gathering and reporting of the vote is unsuccessful. The following steps should be taken to ensure that the voting equipment and the voting process are secure at all times in every precinct:

Chief Judge and Judges:

- Inspect voting machines for physical damage while setting up or closing units and record on maintenance log. Examples: damaged or broken lid hinges, cracked cases, and damage to equipment inside case.
- Record all serial numbers to all voting machines seals.
- Report any suspicious activity in or around voting machines to the county board of elections and/or call 911 if immediate help is required.

4. Warehouse Security:

- Physical security during non-election times
- Protective serial numbered seals
- Limited access

When not in use, all election equipment should be stored in a locked room or warehouse with a single deadbolt lock or secured access system. Access to the warehouse/room should be limited to election officials and authorized technicians and the county security department. The storage facility should be equipped with a 24 hour comprehensive alarm monitoring system which alerts to door openings, motion detection, smoke and fire. The storage area should be climate controlled with maintenance of temperature range and a humidity limit.

An activity log should be maintained to record date, time, staff person, and reason for entering the secured room. All voting machines, voter cartridges, and storage media should be secured in a controlled access room. Staff should maintain a detailed inventory control of these supplies.

Conclusion

Adoption of this voting system security policy will increase the overall security of each county's system as well as the security of the electoral process across the state. Further, it will enhance preparation for the deployment of HAVA-compliant voting equipment in the next several years.

DRAFT