COV VSM Guideline SEC2005-01.1
Date: January 17, 2005
Revision: 0

COMMONWEALTH OF VIRGINIA

Voting System Management Guideline

VOTING SYSTEMS SECURITY GUIDELINES

State Board of Elections

Preface

Publication Designation

COV VSM Guideline SEC2005-01.1

Subject

Voting Systems Security

Effective Date

January 17, 2005

Supersedes

Does not supersede any guideline.

Scheduled Review

One (1) year from effective date

Authority

Code of Virginia, § 24.2-103
(Powers and duties in general of the State Board of Elections)

Code of Virginia, §§ 24.2-625 to 24.2-642
(Voting Equipment and Systems)

COV ITRM Policy 90-1
(Information Technology Security Policy)

COV ITRM Standard SEC2001-01.1
(Information Technology Security Standard)

COV ITRM Guideline SEC2001-01.1
(Information Technology Security Guideline)

COV ITRM Standard SEC2003-02.1
(Information Technology Security Standard)

Scope

This guideline is applicable to all County and City electoral boards, general registrars and officers of election that are engaged in such functions as purchasing, testing, managing, maintaining and operating voting systems.

Purpose

This guideline is published as a complementary document to the Voting Systems Security Standard (i.e., COV VSM Standard SEC2005-01.1). As such, it contains additional security procedures and actions that are strongly recommended, but which are not required as mandatory. Accordingly, this security guideline should be considered:

1. To further strengthen an electoral board's Voting Systems Security Program.
2. To further promote the appropriate protection of voting systems within the Commonwealth.
3. To further facilitate the alignment and adaptation of security safeguards to the operational needs of County and City electoral boards.

General Responsibilities

State Board of Elections
In accordance with the *Code of Virginia, § 24.2-103*, the State Board of Elections is assigned the following duties: "…supervise and coordinate the work of the county and city electoral boards and

of the registrars to obtain uniformity in their practices and proceedings and legality and purity in all elections." The State Board of Elections "shall make rules and regulations and issue instructions and provide information to the electoral boards and registrars to promote the proper administration of election laws."

Secretary of the State Board of Elections
In accordance with the *Code of Virginia*, *§ 24.2-102*, the Secretary of the State Board of Elections "…may employ the personnel required to carry out the duties imposed by this title."

County and City Electoral Boards
In accordance with the *Code of Virginia*, *§ 24.2-109*, the electoral board "…shall perform the duties assigned by this title including, but not limited to, the preparation of ballots, the administration of absentee ballot provisions, the conduct of the election, and the ascertaining of the results of the election."

County and City General, Assistant, and Special Assistant Registrars

In accordance with the *Code of Virginia*, *§ 24.2-114*, the general, assistant, and special assistant registrars shall "Carry out such other duties as prescribed by the electoral board."

County and City Officers of Election
In accordance with the *Code of Virginia*, *§ 24.2-611*, officers of election are sworn to "…perform the duties of this election according to the law and the best of my ability..." and "…studiously endeavor to prevent fraud, deceit, and abuse in conducting this election."

Definitions

See Glossary

Related COV VSM Policies, Standards, and Guidelines

COV VSM Policy SEC2005-01, Voting Systems Security Policy; Dated January 17, 2005

COV VSM Standard SEC2005-01.1, Voting Systems Security Standards; Dated January 17, 2005

COV VSM Self-Assessment Guide SEC2005-01.1, Voting System Security Self-Assessment Guide; Dated January 17, 2005

Table of Contents

Background

This security guideline is published as a complementary document to COV VSM Standard SEC2005-01.1: *Voting Systems Security Standard*. As such, it contains additional security procedures and actions that are strongly recommended, but which are not mandatory. Accordingly, this security guideline should be considered:

- To further strengthen an electoral board's Voting Systems Security Program.
- To further promote the appropriate protection of voting systems within the Commonwealth.
- To further facilitate the adaptation and alignment of security safeguards to the operational needs of County and City electoral boards.

As election laws, elections standards and voting system technology continue to evolve and mature, the State Board of Elections will continue to identify security procedures and actions that enable County and City electoral boards to further strengthen their security safeguards. However, given the diversity of technical and operational environments among the electoral boards across the Commonwealth, it is not always practicable to qualify all security procedures and actions as State Board of Elections voting systems security standards. Thus, several such security procedures and actions are more appropriately qualified as "guidelines". Nonetheless, a large percentage of the County and City electoral boards will find significant value in formally adopting the security procedures and actions listed in this guideline as part of their Voting Systems Security Programs.

Approach

This COV VSM Guideline supports the Voting Systems Security Framework, endorsed by the State Board of Elections, which consists of the following three safeguard types and twelve security safeguard components:

Security Safeguard Type	Security Component
Administrative	Security risk assessment Security awareness and training Security incident handling Security monitoring and review control Security contingency planning Access management
Physical	Physical access controls Environmental controls
Technical	Technical access control Configuration management Testing Network security

Voting Systems Security Framework

These components provide a framework that promotes the appropriate protection of voting systems within the Commonwealth. In addition, they provide the basis for designing the electoral boards' security programs and safeguards. Thus, for each security safeguard component listed above, a subset of security procedures and actions has been identified that, together, comprise this COV VSM Guideline SEC2005-01.1: *Voting Systems Security Guideline*.

Detail descriptions of each security component are presented in COV-VSM SEC2005-01.1: *Voting Systems Security Standard* and will not be repeated by this document. Therefore, since this guideline is intended to complement that standard, it is recommended that the electoral board become familiar with the contents of the standard in order to better understand this guideline.

Reviews

A full annual review of COV VSM Guideline SEC2005-01.1 is anticipated.

Statement of VSM Practices for Voting Systems Security

This section groups the security procedures and actions of COV VSM Guideline SEC2005-01.1: *Voting Systems Security Guideline* by the three security safeguard types and the twelve security safeguard components that comprise the Voting Systems Security Framework.

A. Administrative Security Safeguards

Administrative security safeguards refer to those standards, procedures, and actions taken to manage the selection, development, implementation, and maintenance of security measures to protect voting systems and to manage the conduct of elections personnel in relation to the protection of voting systems.

A.1. Security Risk Assessment

The purpose of a security risk assessment is to identify and evaluate the risks to which a local jurisdiction's voting systems are subject. Based upon the risk assessment the electoral board determines what types of safeguards are appropriate to address the identified risks. In this manner, the administrative, physical, and technical safeguards put in place reflect those security safeguards that are reasonable and appropriate for a local jurisdiction's technical and operational environments. Security safeguards should be referable back to the risk assessment.

A.1.a. Security Procedures and Actions

A.1.a.i. In developing implementing and maintaining a Voting Systems Security Program, each electoral board must keep in mind that voting system security requires ongoing diligence. Environments change over time, whether through moves to new facilities, changes in voting system technology, or changes in election laws. And even if these items do not change, elections personnel do.

Individual Voting Systems Security Programs can be broken down into many different components, but an effective program must always contain the following key components:

- Procedures that outline the proper and improper uses of voting systems.
- Administrative, physical and technical safeguards to protect voting systems and to prevent their misuse.
- Awareness and training programs for all elections personnel.
- Clearly defined roles, authorities, and responsibilities for managing voting systems security.
- Consistently employed systems of checks and balances and routine maintenance of retrievable documentation sufficient to

substantiate the exercise of all due diligence in establishing and maintaining the security of the voting systems utilized.
- Periodic review and evaluation of the program's effectiveness.

A.1.a.ii. Threats, risks or vulnerabilities that could potentially jeopardize the integrity or availability of the voting systems and should be thoroughly considered include but are not limited to:

- Damage, theft or loss.
- Unauthorized access, intrusion into or alteration of hardware, firmware or software.
- Unlawful or unauthorized use of system components.
- Unlawful or unauthorized access to, disclosure, use or manipulation of sensitive or confidential data or private information.
- Interruption of chain of custody, control or accountability.
- Malfunctions or failures that could result in disruption of the election process on Election Day.
- Programming or function errors that could result in the inaccurate recording of votes or reporting of election results.
- Gaps, lapses or inconsistencies in the implementation and enforcement of security mechanisms.

A.1.a.iii. In conducting a security risk assessment to identify the potential security risks to those voting systems for which an electoral board is accountable and to determine the appropriate security safeguards to be implemented to protect these voting systems, an electoral board should use a six-step process similar to the one described below.

- **Step One -** Conduct an inventory of all voting system components to identify the assets involved in the support of the use of voting systems in the elections process.
- **Step Two -** Conduct a threat analysis to identify the potential threats to these assets.
- **Step Three –** Conduct a vulnerability assessment of these assets to identify any asset vulnerabilities that can be exploited.
- **Step Four –** Develop security safeguard recommendations linked to the results of the Steps One, Two and Three.
- **Step Five –** Decide to implement security safeguards based upon their costs and the magnitude of the impact they mitigate.
- **Step Six –** Communicate the results of the risk assessment process to elections personnel and monitor the implementation and compliance with the security safeguards.

A.1.a.iv. In assigning the level of risk, each electoral board should evaluate both the probability of an event occurring and the resultant effect

of that event on the confidentiality, availability, integrity, and functionality of voting systems.

A.1.a.v. Every effort should be made to devise a documentation system, procedure, check or balance measure, testing or maintenance routines, review procedure or other practical safeguard to address the risks or vulnerabilities identified. The effectiveness of devised safeguards will be enhanced if they are supported with:

- Written instructions.
- Pre-planned calendars of scheduled testing, maintenance, monitoring, review routines and reporting activities.
- Design of appropriate manual or electronic logs, spreadsheets or reporting forms for documenting access, asset inventory and movement controls, testing, maintenance, monitoring and review routines, incidents of suspected violations or breaches, upgrades, modifications and changes, and other activities or events related to the security of the voting systems.
- Hard copy or electronic document management or filing systems that ensure the ease of their use and retrieval.

A.1.a.vi. In handling exceptions to any mandatory security standard, it should be remembered that an exception only occurs when an electoral board does not or cannot comply with a mandatory security standard.

Basic exception classification is very simple:

- **Anticipated exceptions** – an occasion where an electoral board, due to environmental considerations, does not choose to or is prevented in some way from complying with a mandatory security standard. A letter-to-file, with a copy to the State Board of Elections, identifying the standard to which the exception applies, the circumstances that make the exception advisable or necessary, a statement of the impact of non-compliance, description of alternative measures that will be implemented, if any, and signed by the Chairman of the Electoral Board is adequate to document such an exception.

- **Unanticipated exceptions** – an occasion where an electoral board, as the result of an unexpected, infrequent and non-repetitive event is prevented in some way from complying with a mandatory security standard. A letter-to-file, with a copy to the State Board of Elections, identifying the standard to which the exception applies, the circumstances surrounding the event that caused the exception, a statement of the impact of non-compliance, a description of the actions being taken by the electoral board to clear the exception and signed by the

Chairman of the Electoral Board is adequate to document such an exception.

A.2. Security Awareness and Training

The purpose of security awareness and training is to promote elections personnel awareness, training and responsibility with respect to security risks, policy, standards, guidelines, and procedures related to the protection of voting systems. All elections personnel within a local jurisdiction need to understand the sensitivity of the jurisdiction's voting systems and their responsibilities in protecting these systems. Security awareness and training programs also provide a proactive mechanism of fostering further comprehension of each individual's responsibilities in sustaining the security of voting systems. Security awareness and training programs are most effective when they are composed of a combination of initial and periodic refresher security training sessions along with on-going security awareness reminders.

A.2.a. Security Procedures and Actions

A.2.a.i. Security awareness programs should contain content that covers, but is not limited to:

- Emphasis that maintenance of the security and integrity of the voting systems is a shared responsibility among all personnel, contractors, and volunteers involved.
- Responsibility of elections personnel to consistently implement security safeguards, abide by security standards, and maintain associated documentation.
- Responsibility of elections personnel to report security issues/incidents.
- Elections personnel can and will be reviewed and monitored.
- Legal requirements for protecting voting systems (citing legislation as appropriate).
- Identification of systems, programming and system information, voter information, votes, results or other data about which there are restrictions as to their use, disclosure, distribution or duplication, as well as privacy and confidentiality expectations required of personnel.
- Discussion of potential threats, risks, vulnerabilities.
- Written instructions related to specific security safeguards that are to be implemented.

A.2.a.ii. Security awareness programs should include a means to promote security awareness on an on-going basis, i.e., supplemental to initial and recurring training (e.g., security awareness flyers, posters, etc.)

A.2.a.iii. Security awareness training content is not static, and should be continuously reviewed and updated by each electoral board as needed to reflect changes in the electoral board's technical and operational environments.

A.3. Security Incident Handling

The purpose of security incident handling is to respond to a suspected or known instance where voting systems security policy, standards, and procedures have been violated and/or a security safeguard has been breached. The handling of security incidents can be politically, managerially, and technically complex and require information and assistance from sources outside the local jurisdiction (e.g., technical specialists, vendor representatives, law enforcement personnel, public affairs personnel, political party representatives, and State Board of Elections representatives).

A.3.a. Security Procedures and Actions

A.3.a.i. Incident response and reporting procedures should detail the steps to be taken by elections personnel to identify, notify, contain, eradicate, recover from, record and report security incidents.

A.3.a.ii. Incident response and reporting procedures related to the handling of suspected violations or breaches in voting system security generally involve the following steps.

1. Establishing general procedures for responding to incidents.
2. Preparing to respond to incidents.
3. Analyzing all available information to characterize an incident.
4. Communicating with all parties that need to be made aware of an incident and progress in its handling.
5. Collecting and protecting of information associated with an incident.
6. Applying short-term solutions to contain an incident.
7. Eliminating all means of vulnerability pertaining to that incident.
8. Returning voting systems to normal operation.
9. Performing a follow-up assessment to ensure that recommendations, maintenance or other remedial measures have been implemented.
10. Bringing about closure by identifying and implementing security lessons learned.

A.3.a.iii. Incidents involving suspected breaches or violations of security may involve coverage by the media. Part of the response strategy should be the development of a plan for dealing with such coverage, should it be forthcoming. The media response plan should include such considerations as:

- An advance determination as to who will be the primary spokesperson.
- Steps that will be taken to ensure that information reported is based on confirmed facts to the greatest extent possible.
- The manner in which a determination will be made as to whether contact with the media about the incident will be initiated internally, or remain solely responsive.
- Whether an official press statement should be released or not.

A.4. Security Monitoring and Review Control

The purpose of security monitoring and review control is to ensure that the implementation and maintenance of security safeguards are adequately documented and managed and that accountability can be established. Security monitoring and review controls also allow responsible officials to verify that security standards and procedures are sustained in a uniform and consistent manner over time. Security safeguards tend to degrade as personnel discover new ways to intentionally or unintentionally bypass security safeguards or simply become lax in their compliance with security procedures. Each electoral board must therefore make risk-based decisions regarding the timing and the scope of follow up, evaluation, walk-through or formal review of security monitoring and review control activities.

A.4.a. Security Procedures and Actions

A.4.a.i. Voting system configurations and software versions change over time. Therefore, each electoral board should review security safeguards (i.e., administrative security safeguards, technical security safeguards, physical security safeguards) on a periodic basis to determine if voting system security standards are being met.

A.4.a.ii. A key element in fulfilling the mandatory security standards is the uniformity and consistency with which established safeguards and procedures are implemented on a day-to-day basis. Monitoring should be a regular and routine part of security management. Incorporating monitoring efforts into the routine should involve the following:

- Assigning responsibility for maintenance or oversight of specific safeguards or processes to specific individuals.
- Whenever appropriate requiring responsible individuals sign and date narrative reports, transaction logs, database reports, evaluations, test and maintenance reports, schedules and other materials related to security activities acknowledging that they have read, reviewed and or approved their content
- Requiring that exceptions or lapses in systematic routines and documentation be noted in writing and that in such instances,

reports to the board include a description of remedial action taken.
- Ensuring that security briefings are part of the agenda for regular meetings of the electoral board.
- Incorporating periodic formal reviews of security documentation and reports by the election board in the official election calendar.
- Conducting random reviews as a means of promoting consistent application of security standards on a day-to-day basis.

A.4.a.iii. Each electoral board should have a voting systems security review performed by a qualified, external reviewing party on a periodic basis as a supplement to internal reviewing activities.

A.5. Security Contingency Planning

The purpose of security contingency planning is to provide for the continued security of voting systems in the event of a disruption in the normal operational environment caused by a voting systems security policy, standard, or procedure having been violated and/or a security safeguard having been breached.

A.5.a. Security Procedures and Actions

A.5.a.i. In developing and maintaining a Security Contingency Plan (SCP), each electoral board should follow the same basic steps. These steps are as follows:

1. Identify situations for which planning is necessary, and if appropriate, prioritize them.
2. Consider the possibility of grouping them in order to reduce duplicative efforts and the amount of planning needed.
3. Consider possible alternative actions.
4. Decide the criteria that will determine which actions should be taken and select the most appropriate action.
5. In planning for a specific type of contingency or situation, divide the actions into three groups: preparatory actions which may be taken prior to the event occurring; actions to be taken if and when the event occurs; and actions necessary if the event does not occur.
6. If possible, causes of the events should be identified and documented. It may be more difficult to identify them if and when the event occurs and while it is happening.
7. If causes of the event have been identified, consider methods for identifying the exact location of the event and a means of remedying it.

8. Consider the possibility that replacement equipment may not be available because of demand from others, because of vendor supply problems, or because vendor installation engineers are not available.
9. Check the availability of electromechanical fail-safe systems / control systems / over-rides, and the effects their operation may have on voting systems.
10. Consider elections personnel requirements.
11. Create documentation for elections personnel to follow in the event of the event occurring.
12. Clearly define the chain of command and the lines of decision-making authority in implementing the contingency plan.
13. Consider the need for "training" all elections personnel on what is expected of them in relation to:
    - The level of their decision-making authority based on their function.
    - The manner and individual to whom they are to report an emergency or contingency situation.
    - Unexpected event occurrences.
    - Generally, events that may require them to take action.
    - Other events which might affect them
14. Consider space requirements. Space may be needed for
    - People (e.g., elections personnel, voters).
    - Voting equipment.
    - Other supplies
15. Arrange escrow agreements with vendors to ensure that their software will be available without delay should it become necessary.

A.3.a.iii. Incidents involving emergencies or imposition of contingency plans may, depending on the severity or magnitude of the incident, require the support of the media to advise the public of the circumstances or changes in locations or services. Media involvement may be helpful, for example, in providing public information in the event a polling station has to be closed down altogether, or there will be a significant interruption of service, or if the emergency involves an authorized extension of polling hours. In planning for public notice related to an emergency or implementation of a contingency plan, the following decisions and development of useful should be considered in advance.

- A determination should be made as to who will be the primary spokesperson or person responsible for releasing the information.
- Criteria should be defined as to kinds of emergencies or contingencies that would benefit from media coverage, the

magnitude of desired coverage that would be appropriate, and which media should be involved.
- A media contact list should be prepared in advance and be easily accessible when needed.
- Steps should be taken to ensure that information or instructions being reported are as complete as possible and based on confirmed facts.
- Statements and releases should be presented in a way that reassures the public that the situation is under control, and promotes the public's confidence in the credibility of the administration and the security and integrity of the election process.

A.6. Access Management

The purpose of access management is to ensure that access to voting systems is consistent with the applicable requirements of Federal and to Commonwealth statutes, State Board of Elections policy and standards, and local electoral board procedures.

A.6.a. Security Procedures and Actions

A.6.a.i. In granting access to voting systems, a mechanism (such as a form, a letter, or an entry on an access authorization listing) needs to be in place to document:

- The necessary details to support the granting of access.
- What privileges an individual is being granted.
- That the granting of access did in fact come from the appropriate authorized person.

A.6.a.ii. In granting access to voting systems, a mechanism (e.g., an identification badge or an authorization letter), should be issued to the person being granted access so that other elections personnel are aware of the person having been granted access.

A.6.a.iii. The periodic review of those granted access to voting systems should include a review of the identity (by name), the defined role (by job description), and location (by local jurisdiction) of the individuals granted access to voting systems.

A.6.a.iv. Should the periodic review of persons granted access to voting systems result in a modification in access status, a mechanism (such as a form, a letter, or an entry on an access authorization listing) needs to be in place to document and notify all elections personnel of the change in access status.

A.6.a.v. Documentation is essential in establishing a review of a log or history of voting systems access management activities. Key steps in the granting, reviewing and modification of access need to be documented. All documented (hard or soft copy) voting systems access management records should be subject to storage and retention requirements as other electoral board documents, and capable of being retrieved in a timely manner.

A.6.a.vi. In granting access to voting systems, it may be necessary for the electoral board to manage exceptions for certain persons (e.g., vendors, visitors) or certain situations (e.g., fire, bomb threat, natural disaster). The electoral board should have developed and implemented procedures that will allow for the granting of access to voting systems in these and other special circumstances.

B. Physical Security Safeguards

Physical security safeguards refer to those standards, procedures, and actions taken to protect voting systems and related facilities and equipment, from natural and environmental hazards, as well as, tampering, vandalism, and theft. Accordingly, physical security safeguards need to be considered for voting systems in storage (e.g., in warehouses), in transit (e.g., being transported between a warehouse and a polling place), in the polling place (e.g., before, on and after election-day), and in use (e.g., during election day). Physical security safeguards provide the primary means of protection for voting systems from natural and environmental hazards, as well as, tampering, vandalism, and theft.

B.1. Physical Access Controls

The purpose of physical access controls is to define the procedures and physical safeguards to control physical access to voting systems and the facility or facilities in which they are housed, while ensuring that personnel granted access by the electoral board are allowed access.

B.1.a. Security Procedures and Actions

B.1.a.i. For those facilities where access is gained through the use of an access code or combination, these codes or combinations should be changed at least every 60 days or in the event of the termination of an individual that previously had access or a relevant change in their status.

B.1a.ii. For those facilities where access is gained through the use of a key, an accounting for all the keys issued for these facilities should be made.

B.1.a.iii. Should it prove impossible to account for all keys issued for a facility or when a key is missing, the locking mechanism should be replaced.

B.1.a.iv. The electoral board should review the effectiveness of physical access controls in each facility where voting systems are housed and stored, both during normal hours of operation and at other times – particularly when a facility may be unoccupied.

B1.a.v. Physical access control violations should be documented reported to higher authority and acted upon in a timely and appropriate manner.

B.2. Environmental Controls

The purpose of environmental controls is to define the procedures and physical safeguards to secure the physical environment in which voting systems must operate and are stored.

B.2.a. Security Procedures and Actions

B.2.a.i. Voting systems should be stored and housed in environmentally friendly facilities (e.g., which includes fire protection, heating, humidity controls, HVAC).

B.2.a.ii. The proper functioning of environmental control systems should be periodically confirmed.

B.2.a.iii. The availability of fire protection and suppression systems should be periodically confirmed and tested.

C. Technical Security Safeguards

Technical security safeguards refer to the technology and the standards and procedures for its use that protect the integrity and security of voting systems and control access to them.

C.1. Technical Access Control

The purpose of technical access control is to implement technology and procedures that control access to voting systems technologies, software, firmware, operating systems and data, only to those persons and software authorized by the electoral board.

C.1.a. Security Procedures and Actions

C.1.a.i. A physical and/or technical inspection should be periodically conducted to confirm that NO voting system components are connected to ANY form of communications network while the polls are open.

C.1.a.ii. For those voting system components that are capable of being password protected, the passwords should be composed of a mixture of letters and numbers, with at least one capital letter.

C.1.a.iii. For those voting system components that are capable of being password protected, the passwords should be at least eight (8) digits long.

C.1.a.iv. For those voting system components that are capable of being password protected, the passwords should be changed at least every 90 days.

C.1.a.v. For all password-protected voting system components that posse an automatic logoff feature, automatic logoff should occur after three (3) failed attempts to enter a correct password.

C.1.a.vi. Password access to voting systems should be terminated IMMEDIATELY when an individual's employment or contract is terminated, or when an individual no longer requires access or when an individual's access status is changed.

C.1.a.vii. For those voting system components that are capable of being password protected, a password should not be reset without physically authenticating the identity of the person requesting that the password be reset and the fact that the person has been granted access to the voting system component.

C.2. Configuration Management

The purpose of configuration management is to implement technology and procedures that control the hardware, firmware, software, and documentation configurations of voting systems so that only those hardware, firmware, and software components that have been qualified by Independent Testing Agencies and certified by the Commonwealth become part of a local jurisdiction's voting systems configurations. Configuration Management essentially consists of four tasks:

- **Identification:** this is the specification, identification of all voting systems components and their inclusion in the Configuration Management Database.
- **Control:** this is the management of each voting systems component, specifying who is authorized to "change" (e.g., modify, move) it and whose approval is required for the "change".
- **Status:** this task is the recording of the status (e.g., modifications, problems, movements, Etc.) of all voting systems components in the Configuration Management Database, and the maintenance of this information.
- **Verification:** this task involves local reviews and third-party reviews (if conducted) to ensure that the information contained in the Configuration Management Database is accurate.

C.2.a. Security Procedures and Actions

C.2.a.i. A Configuration Management Database should include all the information available (e.g., nomenclature, make, model, serial number, date of manufacture, date of purchase, date of failures/problems, date of repairs/fixes, name, address, and telephone number of vendor, name address, and telephone number of person who authorized repair/fix, certification status, location, Etc.) on each uniquely identifiable voting system component.

C.2.a.ii. The Configuration Management Database should maintained in Microsoft Excel or Microsoft Access.

C.2.a.iii. There are three generally accepted methods used for erasing or otherwise making unreadable sensitive information on hard drives or floppy disks:

- **Overwriting:** Overwriting of sensitive means replacing previously stored information on a hard drive or floppy disk with a predetermined pattern of meaningless information. This effectively renders the data unrecoverable, but the process should be correctly understood and carefully implemented. Overwriting or degaussing should be accomplished whenever a voting system is being transferred to another local jurisdiction or is being traded-in with a vendor.
- **Degaussing:** A process whereby the magnetic media are erased using a strong magnet. Properly applied, degaussing renders any previously stored information on the magnetic disks unreadable. Overwriting or degaussing should be accomplished whenever a voting system is being transferred to another local jurisdiction or is being traded-in with a vendor.
- **Physical Destruction:** Hard drives and floppy disks should be physically destroyed when they are defective and cannot be economically repaired or when the voting system has been declared surplus or is being disposed of. Physical destruction should be accomplished to an extent that precludes any possible further use of the hard drive or floppy disk.

C.2.a.iv. Deleting files removes information from storage media in a manner that renders it unreadable unless special utility software or techniques are used to recover the cleared data. However, because the deleting process does not prevent information from being recovered by technical means, it is not considered an acceptable method of removing information from voting system hard disk or floppy disk storage media.

C.3. Testing

The purpose of testing is to implement technology and procedures that demonstrate and confirm to the greatest extent possible that the voting systems in use within a local jurisdiction are identical to the voting systems certified by the State Board of Elections and that the voting system is functioning in a manner that assures the accurate recording of votes and reporting of results.

C.3.a. Security Procedures and Actions

C.3.a.i. The step-by-step procedures that are followed in the conduct of the Logic and Accuracy Testing of each voting system should be documented.

C.3.a.ii. The design of the Logic and Accuracy Test should be directed, supervised and approved by the electoral board.

C.3.a.iii. The results of each Logic and Accuracy Test for each voting system should be documented and signed by an electoral board member and retained for a period of one year.

C.3.a.iv. The step-by-step procedures that are followed in the conduct of the Acceptance Testing of each voting system should be documented.

C.3.a.v. The results of each Acceptance Test for each voting system should be documented and signed by an electoral board member and retained for as long as the electoral board retains possession of the voting system.

C. 3.a.vi. When feasible, notice of the dates on which Logic and Accuracy Testing will be accomplished should be made available to the media and to political parties. In the event there are witnesses to the testing, their presence should be documented.

C.4. Network Security

The purpose of network security is to implement technology and procedures that guard against unauthorized access to voting systems through an electronic communications network (e.g., dial-up, LAN, WAN, Internet, Etc.).

C.4.a. Security Procedures and Actions

C.4.a.i. A physical and/or technical inspection should be periodically conducted to confirm that NO voting system components are connected to ANY form of communications network (e.g., dial-up, LAN, WAN, Internet, Etc.) while the polls are open.

C.4.a.ii. Any approval to connect any voting system component to a communications network of any type, for any purpose other than voting system setup or opening and closing the polls, should be in writing and from the State Board of Elections only. This approval should be retained for as long as the connection is maintained or until the approval is superseded.

Glossary

Acceptance Testing - The purpose of acceptance testing is to demonstrate and confirm to the greatest extent possible that the voting systems purchased or leased by a local jurisdiction are identical to the voting systems certified by the State Board of Elections and that the voting systems equipment and software is fully functional and capable of satisfying the administrative and statutory requirements of the local jurisdiction. Acceptance testing is conducted when voting systems are initially received by the local electoral board from a vendor or other outside source (e.g., another local jurisdiction).

Access Control - The purpose of access control is to implement technology and procedures that control access to voting systems only to those persons and software authorized by the Chairman of the electoral board and/or the general registrar. The entire subject of voting systems security is based upon access control, without which voting systems security cannot, by definition, exist.

Access Management - The purpose of access management is to ensure that access to voting systems is consistent with the applicable requirements of Federal and to Commonwealth statutes, State Board of Elections policy and standards, and local electoral board procedures.

Administrative Safeguards - Those standards, procedures, and actions taken to manage the selection, development, implementation, and maintenance of security measures to protect voting systems and to manage the conduct of elections personnel in relation to the protection of voting systems.

Alteration - Any physical intrusion into voting system hardware or installation of non-certified software.

Authentication - Authentication refers to the verification of the authenticity of a person's identity. Authentication techniques usually form the basis for all forms of access control to voting systems.

Authorization - The process whereby the Chairman of the electoral board or general registrar approves a specific action or approves the granting of access to voting system components for a specific individual.

Authorized Personnel – Those individuals granted access to voting system components by an electoral board.

Availability - Ensuring that voting systems and the necessary supporting components are available for use when they are needed.

Best Practice - A management or technical policy, standard, guideline, procedure or practice that has consistently been shown to improve the security of information technology resources.

Certification Testing - The purpose of certification testing is to verify that the design and performance of the voting system being tested comply with all of the requirements of the *Code of Virginia*. Certification testing is not intended to exhaustively test all of the voting system hardware and software attributes; these are evaluated during qualification testing. However, all voting system functions, that are essential to the conduct of an election, are evaluated.

Configuration Management - The purpose of configuration management is to implement technology and procedures that control the hardware, firmware, software, and documentation configurations of voting systems so that only those hardware, firmware, and software components that have been qualified by Independent Testing Agencies and certified by the Commonwealth become part of a local jurisdiction's voting systems configurations.

Configuration Management Database - An electronic or non-electronic permanent record of all required configuration management data associated with all voting system components for which a local jurisdiction is accountable.

Confidentiality - Assurance that information is shared only among authorized persons or organizations. Breaches of Confidentiality can occur when data is not handled in a manner adequate to safeguard the confidentiality of the information concerned. Such disclosure can take place by word of mouth, by printing, copying, e-mailing or creating documents and other data etc. The classification of the information should determine is confidentiality and hence the appropriate safeguards.

Control (CM) - The management of each voting systems component, specifying who is authorized to "change" (e.g., modify, move) it and whose approval is required for the "change".

Elections Personnel - All personnel employed or appointed/designated to support the testing, preparation, operation, movement, or storage of voting systems.

Environmental Controls - The purpose of environmental controls is to define the procedures and physical safeguards to secure the physical environment in which voting systems must operate and are stored.

House - To place voting systems in a facility when in use.

Identification (CM) - The specification and identification of all voting system components and their inclusion in a Configuration Management Database.

Independent Testing Authority - Companies selected by the National Association of State Election Directors (NASED) or the National Institute of Standards and Technology (NIST) to conduct qualification testing for voting systems."

Information Security Principles –

1. Voting systems are critical and vital assets to the Commonwealth.

2. These assets require a degree of protection commensurate with their value (material and non-material) to the Commonwealth.

3. Measures should be taken to protect these assets against accidental or unauthorized disclosure, alteration or destruction, as well as to assure their security, reliability, integrity and availability.

4. The protection of assets is a management responsibility.

5. Access to voting systems must be strictly controlled.

6. Information that is sensitive or confidential must be protected from unauthorized access or alteration.

7. Voting system components that are essential to the proper functioning of voting systems must be protected from theft, vandalism, tampering, alteration, loss or destruction.

8. Risks to voting systems must be managed. The expense of security safeguards must be appropriate to the value of the assets being protected.

9. The integrity of voting system software must be assured. Changes to software must be made only in authorized and acceptable ways.

10. Security needs must be considered and addressed in all phases of elections operations.

11. Security awareness and training of elections personnel is one of the most effective means of reducing vulnerability to security risks and must be continually emphasized and reinforced. All elections personnel must be accountable for their actions relating to voting systems.

12. Voting Systems Security Programs must be responsive and adaptable to changing operational and environmental vulnerabilities and technologies.

Integrity - Assurance that voting system components are authentic and complete.

LAN (Local Area Network) - A computer network that covers a relatively small area. Most LANs are kept to a single building or group of buildings. However, one LAN can be connected to other LANs over any distance via telephone lines and radio waves.

Logic and Accuracy Testing - The purpose of logic and accuracy testing is to demonstrate and confirm to the greatest extent possible that the voting systems in use within a local jurisdiction are identical to the voting systems certified by the State Board of Elections and accepted by the local electoral board. Logic and accuracy testing is conducted before and after each election.

Network Security - The purpose of network security is to implement technology and procedures that guard against unauthorized access to voting systems through an electronic communications network (e.g., dial-up, LAN, WAN, Internet, Etc.).

Physical Access Controls - The purpose of physical access controls is to define the procedures and physical safeguards to control physical access to voting systems and the facility or facilities in which they are housed, while ensuring

that properly authorized personnel are allowed access.

Physical Safeguards - Those standards, procedures, and actions taken to protect voting systems and related facilities and equipment, from natural and environmental hazards, as well as, tampering, vandalism, and theft.

Qualification Testing - The purpose of qualification testing is to demonstrate that the voting system complies with the requirements of its own design specifications. This testing encompass selective in-depth examination of software; inspection and evaluation of voting system documentation; tests of hardware under conditions simulating the intended storage, operation, transportation, and maintenance environments; and tests to verify system performance and function under normal and abnormal operating conditions. An Independent Testing Authority (ITA) normally conducts qualification testing.

Security Awareness and Training - The purpose of security awareness and training is to promote Elections Personnel awareness, training and responsibility with respect to security risks, policy, standards, guidelines, and procedures related to the protection of voting systems.

Security Breach - Any event or action that compromises the security, confidentiality, integrity or availability of voting systems and the elections process they support.

Security Contingency Planning - The purpose of security contingency planning to provide for the continued security of voting systems in the event of a disruption in the normal operational environment caused by a voting systems security policy, standard, or procedure having been violated and/or a security safeguard having been breached. A secondary purpose of security contingency planning is to minimize the effect of such disruptions.

Security Incident - Any act or circumstance involving classified information that deviates from the requirements of governing security publications. For example, compromise, possible compromise, inadvertent disclosure, and deviation.

Security Incident Handling - The purpose of security incident handling is to respond to a suspected or known instance where voting systems security policy, standards, and procedures have been violated and/or a security safeguard has been breached.

Security Monitoring and Review Control - The purpose of security monitoring and review control is to ensure that the implementation and maintenance of security safeguards are adequately documented and managed and that accountability can be established.

Security Risk Assessment - The purpose of security risk assessment is to identify and evaluate the risks to which a local jurisdiction's voting systems are exposed.

Status (CM) - The management of each voting systems component, specifying who is authorized to "change" (e.g.,

modify, move) it and whose approval is required for the "change".

Store – To place voting systems in a facility when not in use.

Technical Safeguards - The technology and the standards and procedures for its use that protect voting systems and control access to them.

Testing - The purpose of testing is to implement technology and procedures that demonstrate and confirm to the greatest extent possible that the voting systems in use within a local jurisdiction are identical to the voting systems certified by the State Board of Elections. Acceptance Testing is conducted when voting systems are initially received from a vendor or other outside source (e.g., another local jurisdiction). Logic and Accuracy Testing is conducted before and after each election.

Third-party - A party other than an electoral board member or another election official, such as a County or City auditor or a private contractor, providing independent assessment or audit services.

Verification (CM) - The local review and/or third-party review to ensure that the information contained in a Configuration Management Database is accurate.

Voting System - The term "voting system" refers to the total combination of mechanical, electro-mechanical and electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment) that is used to: define ballots; cast and count votes; report or display election results; and to maintain and produce any review trail information; and the practices and associated documentation used to: identify voting system components and versions of such components; test the system during its development and maintenance; maintain records of system errors and defects; to determine specific system changes to be made a system after the initial qualification of the system; and make available any materials to the voter (such as notices, instructions, forms, or paper ballots).

WAN (Wide Area Network) - A communications network that covers a wide geographic area, such as a city, county or state. It usually consists of several LANs.

Notes