Mapping of VVSG 2007 Access Control Requirements to VVSG Cybersecurity Working Group Principles and Guidelines

This information is based on the requirements found at:
http://collaborate.nist.gov/voting/pub/Voting/CyberSecurity/2007-VVSG.pdf

5.4 Access Control

The purpose of access controls is to limit the rights of authorized users, applications, or processes and prevent unauthorized use of a resource or use of a resource in an unauthorized manner. The core components of access control include identification, authentication, enforcement, and policy. Access control mechanisms authenticate, authorize, and log access to resources to protect voting system integrity, availability, confidentiality, and accountability. The intent of the standard is that access controls should provide reasonable assurance that voting system resources such as data files, application programs, underlying operating systems, and voting system devices are protected against unauthorized access, operation, modification, disclosure, loss, or impairment.

This section addresses voting system capabilities that limit and detect access to critical voting system components in order to guard against loss of system and data integrity, availability, confidentiality, and accountability in voting systems. Access controls may be implemented in the voting software or provided by the underlying operating system or separate application programs.

Access controls include physical controls, such as keeping voting devices in locked rooms to limit physical access, and technical controls, such as security software programs designed to prevent and detect unauthorized access to resources.

5.4.1 General Access Control

General requirements address the high-level functionality of a voting system. These are the fundamental access control requirements upon which other requirements in this section are based.

4.2.1-A Access control mechanisms

Requirement:	The voting device SHALL provide access control mechanisms designed to permit authorized access to the voting system and to prevent unauthorized access to the voting system.
Applies to:	Voting system
Test Reference:	Part 3:5.2 “Functional Testing”

Discussion:	Access controls support the following security principles in terms of voting systems: 1. Accountability of actions by identifying and authenticating users; 2. Confidentiality of casting and storing of votes; 3. Integrity of event logs, electronic records, and vote reporting; and 4. Availability of the voting ballot and the ability to cast, store, and 1. report votes. This requirement extends [VVSG2005] I.7.2.1.2 by requiring controlled access to voting device components and by requiring access control mechanisms
Source:	[VVSG2005] I.7.2.1.2-1, I.7.2.1.2-2
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations. **Justification:** Although "strong" and "configurable" mechanisms are not mentioned in this requirement, this guideline maps best/

5.4.1-A.1 Voting device access control

Requirement:	The access control mechanisms of the voting device SHALL be capable of identifying and authenticating roles from Part 1:Table 5-1 permitted to perform operations on the voting device.
Applies to:	Voting device
Test Reference:	Part 3:4.5 "Source Code Review", 5.2 "Functional Testing"
Discussion:	Part 1:Table 5-1 provides the roles that must be supported by the voting device. Role-based identification identifies users, applications, and processes based on roles in an organization. Each role has defined permissions within the voting system. Users may authenticate to the voting system using a user account, then assume a role. Accountability is provided for each role within the voting system. The role-based access control method uses rules to define permissions.
Source:	New requirement
Principle(s)/ Guideline(s):	*Security: Access Control* *Principle:* The voting system authenticates administrators, users, devices, and services before granting access to sensitive functions. *Guideline:* The voting system limits the access of users, roles, and processes to the specific functions and data to which each entity holds authorized access. *Guideline:* Default access control policies enforce the principles of least privilege and separation of duties. **Justification:** Due to the old guideline's removal, there may be a gap in our current Access Control Guidelines. The ability to identify and assign roles is not specifically mentioned in our current guidelines.

Table 5-1 Voting system minimum groups and roles

GROUP OR ROLE	DESCRIPTION
Voter	The voter role is a restricted process in the vote-capture device. It allows the vote-capture device to enter the Activated state for voting activities.
Election Judge	The election judge has the ability to open the polls, close the polls, handle fled voters, recover from errors, and generate reports.
Poll Worker	The poll worker checks in voters and activates the ballot style.
Central Election Official	The central election official loads ballot definition files.
Administrator	The administrator updates and configures the voting devices and troubleshoots system problems.

5.4.1-A.2 EMS access control

Requirement:	The access control mechanisms of the EMS SHALL be capable of identifying and authenticating individuals permitted to perform operations on the EMS
Applies to:	EMS
Test Reference:	Part 3:4.5 “Source Code Review”, 5.2 “Functional Testing”
Discussion:	Identity-based identification explicitly identifies a user, application, or process by the use of a unique system-wide identifier, such as an account. Each identity has defined permissions in the voting system. Accountability is provided for each identity within the voting system. Identity-based access control methods use rules to define permissions. Rules may be used in a voting system to provide access policies for identity-based access control.
Source:	New requirement
Principle(s)/ Guideline(s):	*Security: Access Control* *Principle:* The voting system authenticates administrators, users, devices, and services before granting access to sensitive functions. *Guideline:* The voting system limits the access of users, roles, and processes to the specific functions and data to which each entity holds authorized access. **Justification:** The principle and the second guideline align with the identifying and authenticating of individuals.

5.4.1-B Access control for software and files

Requirement:	The voting device SHALL provide controls that permit or deny access to the device’s software and files.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	A voting device’s software includes voting application software and third party software such as the operating system, drivers, and databases. This requirement

	extends [VVSG2005].
Source:	[VVSG2005] I.7.2.1.2-1
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system limits the access of users, roles, and processes to the specific functions and data to which each entity holds authorized access. **Justification:** With the capability to permit or deny access, this requirement follows this guideline by limiting access to software and files.

5.4.1-C Access control voting states

Requirement:	The vote-capture device's access control mechanisms SHALL distinguish at least the following voting states from Part 1:Table 5-2: a. Pre-voting; b. Activated; c. Suspended; and d. Post-voting
Applies to:	Vote-capture device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	Part 1:Table 5-2 shows the minimum states based on Part 1 Sections 8.1 and 8.2. See Part 1 Section 8.2 for additional description of the voting states for vote-capture devices.
Source:	[VVSG2005] I.7.2.1,I.7.2.1.1
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system limits the access of users, roles, and processes to the specific functions and data to which each entity holds authorized access **Justification:** This guideline may need to be amended to include, "during the correct voting state."

Table 5-2 Vote-capture device minimum states

STATE	DESCRIPTION
Pre-voting	Power-on, loading and configuring device software, maintenance, loading election-specific files, preparing for election day usage.
Activated	Activating the ballot, printing, casting, spoiling the ballot.
Suspended	Entered when an election official suspends voting.
Post-voting	Closing polls, tabulation, printing records, power-off.

5.4.1-D Access control state policies

Requirement:	The vote-capture device SHALL allow the administrator group or role to configure different access control policies available in each voting state.
Applies to:	Vote-capture device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	Activated state should offer a strict subset of functions limited to voting only. Prevoting and post-voting states and other defined states may be used for other

	functions such as defining the ballot, collecting votes, updating software, and performing other administrative and maintenance functions. For more examples, see Part 1:Table 5-3. This requirement extends [VVSG2005] I. 7.2 by establishing vote-capture device policies for each voting state in relation to access control.
Source:	[VVSG2005] I.7.2.1.1
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations. The voting system limits the access of users, roles, and processes to the specific functions and data to which each entity holds authorized access **Justification:** The authentication mechanisms are configurable. This requirement allows the administrators to configure these mechanisms. The second guideline mentioned limits access based on the voting state.

5.4.1-E Minimum permissions default

Requirement:	The voting device's default access control permissions SHALL implement the minimum permissions needed for each role or group
Applies to:	Voting device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	Minimum permissions restrict the group or role to access only the information and resources that are necessary for its purpose. This requirement extends [VVSG2005] I. 7.2.1.1 and I.7.2.1.2 by requiring minimum default access control permissions.
Source:	[VVSG2005] I.7.2.1.1, I.7.2.1.2-1
Principle(s)/ Guideline(s):	*Security: Access Control* Default access control policies enforce the principles of least privilege and separation of duties. **Justification:** This requirement imposes least privilege by designating default access to implement the minimum permissions.

5.4.1-F Privilege escalation prevention

Requirement:	The voting device SHALL prevent a lower-privilege process from modifying a higher-privilege process
Applies to:	Voting device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	This requirement extends [VVSG2005] I.7.2.1 by preventing unauthorized process modification
Source:	VVSG [VVSG2005] I.7.2.1 and [VVSG2005] II.6.4.1
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system limits the access of users, roles, and processes to the specific functions and data to which each entity holds authorized access. *Security: System Integrity*

	The voting system limits its attack surface by reducing unnecessary code, data paths, physical ports, and by using other technical controls. **Justification:** These two guidelines assist in preventing lower-privilege process from interacting with a higher-privilege process.

5.4.1-G Privileged operations authorization

Requirement:	The voting device SHALL ensure that an administrator authorizes each privileged operation.
Applies to:	Voting device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	This requirement extends [VVSG2005] I.7.2 by requiring authorization of privileged operations.
Source:	[VVSG2005] I.7.2.1 and [VVSG2005] II.6.4.1
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations. **Justification:** This guideline verifies that the administrator can authorize critical operations.

5.4.1-H Software and firmware modification prevention

Requirement:	The voting device SHALL prevent modification to or tampering with software or firmware through any means other than the documented procedure for software upgrade.
Applies to:	Voting device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	This requirement is intended to ensure that there are no ways, other than the documented procedure for software upgrade, to upgrade or modify the software. This requirement aims to protect against software vulnerabilities that would allow an unauthorized individual to secretly update, modify, or tamper with the installed software. This requirement extends [VVSG2005] I.7.2 by requiring prevention of modification and tampering with software and firmware.
Source:	[VVSG2005] I.7.2.1 and [VVSG2005] II.6.4.1
Principle(s)/ Guideline(s):	*Security: System Integrity* The voting system maintains and verifies the integrity of software, firmware, and other critical components. **Justification:** This requirement belongs under the system integrity section.

5.4.2 Access control identification

Identification requirements provide controls for accountability when operating and administering a voting system. Identification applies to users, applications, and processes.

5.4.2-A Access control identification

Requirement:	The voting device SHALL identify users, applications, and processes to which access is granted and the specific functions and data to which each entity holds authorized access.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	This requirement updates [VVSG2005] I.7.2.1.1-a by requiring that the voting device identify users, applications, and processes. It also requires that identification use either identity-based or role-based methods.
Source:	[VVSG2005] I.7.2.1.1
Principle(s)/ Guideline(s):	*Security: Access Control* Access privileges, accounts, activities, and authorizations are logged, monitored, and reviewed periodically and modified as needed. **Justification:** This guideline covers the establishment of

5.4.2-B Role-based access control standard

Requirement:	Voting devices that implement role-based access control SHALL support the recommendations for Core RBAC in the ANSI INCITS 359-2004 American National Standard for Information Technology – Role Based Access Control document
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	This requirement extends [VVSG2005] I. 7.2.1.1-a by requiring role-based methods to follow ANSI INCITS 359-2004.
Source:	[VVSG2005] I.7.2.1.1
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system authenticates administrators, users, devices, and services before granting access to sensitive functions **Justification:** The principle description describes identifying and authenticating users before granting access to system functions.

5.4.2-C Access control roles identification

Requirement:	The voting device SHALL identify, at a minimum, the groups or roles outlined in Part 1:Table 5-1.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	A group in a voting system is defined as a set of users, applications, or processes who share the same set of privileges and access permissions. In role-based access control methods a role serves the same purpose as a group. In identity

	based access control methods groups are created, members are assigned to the groups, and permissions and privileges are applied to the group as a whole. The term groups and roles are often used interchangeably. provides example activities for each role and is not meant to include all activities performed by each role. This requirement extends [VVSG2005] I.7.2.1.1-a by establishing minimum group or role categories. It also allows each category to apply to different voting states of operation and perform different functions.
Source:	VVSG [VVSG2005] I.7.2.1.1
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system identifies users, roles and/or processes to which access is granted and the specific functions and data to which each entity holds authorized access. **Justification:**

5.4.2-D Group member identification

Requirement:	The EMS SHALL individually identify the members within all groups or roles except the voting group.
Applies to:	EMS
Test Reference:	Part 3:4.4 “Manufacturer Practices for Quality Assurance and Configuration Management”
Discussion:	This requirement extends [VVSG2005] I.7.2.1.1-a by requiring members of groups or roles to be identified explicitly.
Source:	[VVSG2005] I.7.2.1.1
Principle(s)/ Guideline(s):	**Access Control** The voting system identifies users, roles and/or processes to which access is granted and the specific functions and data to which each entity holds authorized access.

5.4.2-E Access control configuration

Requirement:	The voting device SHALL allow the administrator group or role to configure the permissions and functionality for each identity, group or role to include account and group/role creation, modification, and deletion.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	For vote-capture devices, each group/role may or may not have permissions for every voting state. Additionally the permissions that a group/role has for a voting state may be restricted to certain functions. Part 1:Table 5-3 shows an example matrix of group or role to voting state access rights; the table is not meant to include all activities. This requirement extends [VVSG2005] I.7.2.1.1-a by allowing configuration flexibility for permissions and functionality for each identity, group, or role.
Source:	VVSG2005] I.7.2.1.1
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system supports strong, configurable authentication mechanisms to

verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations
Justification: This guideline allows the authentication mechanisms to be configured.

Table 5-3 Roles and voting states access matrix

ROLE	PRE-VOTING	ACTIVATED	SUSPENDED	POST-VOTING
Voter	N/A	Cast and cancel ballots	N/A	N/A
Election Judge	Open polls	Close polls, enter suspended state, handle fled voters, and recover from errors	Exit suspended state	Generate reports
Poll Worker	N/A	Activate ballot	N/A	N/A
Central Election Official	Define and load ballot	N/A	N/A	Reconcile Provisional-challenged ballots, write-ins, Generate reports
Administrator	Full access	Full access	Full access	Full access
Application or Process	Custom per application or process	Custom per application or process	Custom per application or process	Custom per application or process

5.4.3 Access control authentication

Authentication establishes the validity of the identity of the user, application, or process interacting with the voting device. Authentication is based on the identification provided by the user, application, or process interacting with the voting device. User authentication is generally classified in one of the following three categories:

(a) Something the user knows – this is usually a password, pass phrase, or PIN
(b) Something the user has – this is usually a token that may be either hardware or software based, such as a smart card
(c) Something the user is – this is usually a fingerprint, retina patter, voice pattern or other biometric data

Traditional password authentication is a single factor authentication method. A more secure method of authentication combines the various methods of authentication into two-factor authentication, or multi-factor authentication. For example, a user may use a authentication token and a passphrase for authentication. Using multi-factor provides stronger authentication than single factor. There are also cryptographic-based authentication methods such as digital signatures and challenge-response authentication, which are either software or hardware-based based tokens. Applications and processes use programmatic methods of authentication such as digital signatures and certificates.

5.4.3-A Minimum authentication mechanism

Requirement:	The voting device SHALL authenticate users per the minimum authentication methods outlined in Part 1:Table 5-4.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	Part 1:Table 5-4 provides the minimum authentication methods required for each group or role. Stronger authentication methods than the minimum may be used for each group or role. This requirement extends [VVSG2005] I.7.2.1.2-e by requiring a minimum level of robustness for user authentication mechanisms.
Source:	[VVSG2005] I.7.2.1.2-1
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations **Justification:** This guideline discusses the authentication mechanism supported by the voting system and the table mention in this guideline should be reviewed.

5.4.3-C Administrator group or role multi-factor authentication

Requirement:	The voting device SHALL authenticate the administrator group or role with a multi-factor authentication mechanism.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”

Discussion:	This requirement extends [VVSG2005] I.7.2.1.2-e by requiring multi-factor authentication for the voting device administrator group or role.
Source:	[VVSG2005] I.7.2.1.2-1
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms f*or* critical operations **Justification:** This requirement discusses multi-factor authentication mechanisms as mentioned in this guideline.

Table 5-4 Minimum authentication methods for groups and roles

GROUP OR ROLE	MINIMUM AUTHENTICATION METHOD
Election Judge	User name and password
Poll Worker	N/A – poll worker does not authenticate to voting system
Central Election Official	User name and password
Administrator	Two-factor authentication
Application or Process	Digital certificate or signature

5.4.3-D Secure storage of authentication data

Requirement:	When private or secret authentication data is stored in the voting device, the data SHALL be protected to ensure that the confidentiality and integrity of the data is not violated
Applies to:	Voting device
Test Reference:	Part 3:4.5 “Source Code Review”, 5.2 “Functional Testing”
Discussion:	Ensuring the privacy and secrecy of stored data may involve the use of encryption. This requirement extends [VVSG2005] I.7.2.1.2-g by requiring securely stored private or secret authentication data.
Source:	[VVSG2005] I.7.2.1.2-1
Principle(s)/ Guideline(s):	*Security: Data Protection* The voting system protects sensitive data from unauthorized access, modification, or deletion. **Justification:** This requirement belong under the data protection section.

5.4.3-E Setting and changing of passwords, pass phases, and keys

Requirement:	The voting device SHALL allow the administrator group or role to set and change passwords, pass phrases, and keys.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	This requirement support jurisdictions have different policies regarding passwords, pass phrases, and keys. This requirement extends [VVSG2005] I.7.2.1.2-e by allowing the administrator group or role flexibility in creation and modification of passwords, pass phrases, and keys.

Source:	[VVSG2005] I.7.2.1.2-1
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations. **Justification:** This guideline allows the authentication mechanism to be configurable so the administrator can modify passwords, pass phrases, and keys.

5.4.3-F Creation and disabling of privileged groups or roles

Requirement:	The voting device SHALL allow privileged groups or roles to be disabled and allow new individual privileged groups or roles to be created.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	Privileged accounts include any accounts within the operating system, voting device software, or other third party software with elevated privileges such as administrator, root, and maintenance accounts. This requirement extends [VVSG2005] I.7.2.1.2 by allowing the creation and disabling of privileged accounts.
Source:	[VVSG2005] I.7.2.1.2-1
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations. **Justification:** This guideline allows the authentication mechanism to be configurable so the administrator can modify groups and roles, and their privileges.

5.4.3-G Account lock out

Requirement:	The voting device SHALL lock out groups, roles, or individuals after a specified number of consecutive failed authentications attempts within a pre-defined time period.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	This requirement extends [VVSG2005] I.7.2.1.2 by allowing the administrator group or role flexibility in configuring the account lockout policy.
Source:	[VVSG2005] I.7.2.1.2-1
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations. **Justification:** This guideline allows the authentication mechanism to be configured.

5.4.3-H Account lock out configuration

Requirement:	The voting device SHALL allow the administrator group or role to configure the account lock out policy including the time period within which failed attempts

	must occur, the number of consecutive failed access attempts allowed before lock out, and the length of time the account is locked out.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	This requirement extends [VVSG2005] I.7.2.1.2 by allowing the administrator group or role flexibility in configuring the account lockout policy.
Source:	[VVSG2005] I.7.2.1.2-1
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations. **Justification:** This guideline allows the authentication mechanism to be configured.

5.4.3-I User name and password management

Requirement:	If the voting device uses a user name and password authentication method, the voting device SHALL allow the administrator to enforce password strength, histories, and expiration.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	This requirement extends [VVSG2005] I.7.2.1.2-e by requiring strong passwords, password histories, and password expiration.
Source:	[VVSG2005] I.7.2.1.2-1
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations. Justification: This guideline allows the authentication mechanism to be configured.

5.4.3-I.1 Password strength configuration

Requirement:	The voting device SHALL allow the administrator group or role to specify password strength for all accounts including minimum password length, use of capitalized letters, use of numeric characters, and use of nonalphanumeric characters per NIST 800-63 Electronic Authentication Guideline standards.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	This requirement extends [VVSG2005] I.7.2.1.2-e by allowing the administrator group or role flexibility in configuring password strength. It also requires the use of NIST 800-63 standards.
Source:	[VVSG2005] I.7.2.1.2-1
Principle(s)/	*Security: Access Control*

Guideline(s):	The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations. Justification: This guideline allows the authentication mechanism to be configured.

5.4.3-1.2 Password history configuration

Requirement:	The voting device SHALL enforce password histories and allow the administrator to configure the history length.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	Password histories are a log of previously used passwords for automatic comparison with a new chosen password. The password history is used to ensure that recently used passwords are not used again within a pre-defined number of password changes (i.e., history length). This requirement extends [VVSG2005] I.7.2.1.2-e by allowing the administrator group or role flexibility in configuring password history.
Source:	[VVSG2005] I.7.2.1.2-1
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations. **Justification:** This guideline allows the authentication mechanism to be configured.

5.4.3-I.3 Account information for password restriction

Requirement:	The voting device SHALL ensure that the username is not used in the password.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	This requirement extends [VVSG2005] I.7.2.1.2-e by restricting the use or usernames and related information in passwords.
Source:	[VVSG2005] I.7.2.1.2-1
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations. **Justification:** This guideline allows the authentication mechanism to be configured.

5.4.3-I.4 Automated password expiration

Requirement:	The voting device SHALL provide a means to automatically expire passwords in accordance with the voting jurisdiction's policies.
Applies to:	Voting device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	Jurisdiction policies often expire passwords after each election. This requirement extends [VVSG2005] I.7.2.1.2-e by requiring the expiration of unchanged passwords.
Source:	[VVSG2005] I.7.2.1.2-1
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations. **Justification:** This guideline allows the authentication mechanism to be configured.

5.4.4 Access control authorization

Authorization is the process of determining access rights based on authentication of a user, application, or process within a voting device. Authorization permits or denies access to an object by a subject. Subjects may be users, applications, or processes that interact with the voting device. Objects may be files or programs within the voting device.

5.4.4-A Account access to election data authorization

Requirement:	The voting device SHALL ensure that only authorized roles, groups, or individuals have access to election data
Applies to:	Voting device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	This requirement extends [VVSG2005] I.7.2.1.2-a by restricting access to election data to authorized accounts.
Source:	[VVSG2005] I.7.2.1.2-1
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system limits the access of users, roles, and processes to the specific functions and data to which each entity holds authorized access.

5.4.4-B Separation of duties

Requirement:	The voting device SHALL enforce separation of duty across subjects based on user identity, groups, or roles.
Applies to:	Voting device

Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	This requirement extends [VVSG2005] I.7.2.1.2 by requiring separation of duty.
Source:	[VVSG2005] I.7.2.1.2-1
Principle(s)/ Guideline(s):	**Access Control** The voting system authenticates administrators, users, devices and services before granting access to sensitive functions

5.4.4-C Dual person control

Requirement:	The voting device SHALL provide dual person control for administrative activities.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	This requirement extends [VVSG2005] I.7.2.1.2-a by requiring dual person control for administrative activities.
Source:	[VVSG2005] I.7.2.1.2-1
Principle(s)/ Guideline(s):	

5.4.4-D Explicit authorization

Requirement:	The voting device SHALL explicitly authorize subjects’ access based on access control lists or policies.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	This requirement extends [VVSG2005] I.7.2.1.2-a by requiring explicit authorization of subjects based on access control policies.
Source:	[VVSG2005] I.7.2.1.2-1
Principle(s)/ Guideline(s):	

5.4.4-E Explicit deny

Requirement:	The voting device SHALL explicitly deny subjects access based on access control lists or policies.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	This requirement extends [VVSG2005] I.7.2.1.2-a by requiring explicit denying of subjects access based on access control policies.
Source:	[VVSG2005] I.7.2.1.2-1
Principle(s)/ Guideline(s):	**Access Control** Default access control policies enforce the principle of least privilege.

5.4.4-F Authorization limits

Requirement:	The voting device SHALL limit the length of authorization to a specific time,

	time interval, or voting state.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	This requirement extends [VVSG2005] I.7.2.1.1-b by requiring limitations on authorization by time or voting state.
Source:	[VVSG2005] I.7.2.1.2-1
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations. **Justification:** This guideline allows the length of authorization to be configured.