Principle 11
Access Control

The voting system authenticates administrators, users, devices, and services before granting access to sensitive functions.

Requirements for Principle 11

Principle 11 Access Control The voting system authenticates administrators, users, devices, and services before granting access to sensitive functions.

11.1 - Access privileges, accounts, activities, and authorizations are logged, monitored, and reviewed periodically and modified as needed.

11.1-A – Logging activities and resource access

11.1-B – Voter information in log files

11.1-C – No disabling logging

11.1-D – On-demand access to logs

11.2 - The voting system limits the access of users, groups or roles, and processes to the specific functions and data to which each entity holds authorized access.

11.2.1 – Authorized access

11.2.1-A – Ensuring authorized access

11.2.1-B – Modifying authorized user lists

11.2.1-C – Access control by voting stage

11.2.1-D – Access control configuration

11.2.1-E – Administrator modified permissions

11.2.1-F – Authorized assigning groups or roles

11.2.2 – Role-based access control

11.2.2-A – Role-based access control standard

11.2.2-B – Minimum groups or roles

11.2.2-C – Minimum group or role permissions

11.2.2-D – Applying permissions

11.3 - The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations.

11.3.1 – Access control mechanism

11.3.1-A – Access control mechanism application

11.3.1-B – Multi-factor authentication for critical operations

11.3.1-C – Multi-factor authentication for administrators

11.3.2 – Username and password

11.3.2-A – Username and password management

11.3.2-B – Password complexity

11.3.2-C – Minimum password complexity

11.3.2-D – Usernames within passwords

11.4 - Default access control policies enforce the principles of least privilege and separation of duties.

11.4-A – Least privilege for access policies

11.4-B – Separation of duties

11.5 - Logical access to voting system assets are revoked when no longer required.

11.5-A – Access time period

11.5-B – Account lockout

11.5-C – Lockout time duration

11.1 - Access privileges, accounts, activities, and authorizations are logged, monitored, and reviewed periodically and modified as needed.

11.1-A – Logging activities and resource access

The voting system must log any access to, and activities performed on, the voting system, including:

1. timestamps for all log entries
2. all failed and successful attempts to access the voting system
3. all events which change the access control system including policies, privileges, accounts, users, groups or roles, and authentication methods.

Discussion

In the event of an error or incident, the user access log can assist in narrowing down the reason for the incident or error.

- Timestamped log entries will allow for easy auditing and review of access to the voting system.
- Access control logging supports accountability of actions by identifying and authenticating users.
- Groups are a collection of users that are assigned a specific set of permissions. Roles are an identity that is given specific permissions and can be assigned to a user. Any changes to the permissions assigned to groups and roles should be logged to identify updates to a user's privileges.

Prior VVSG source: 2007 VVSG 4.2.1-A

11.1-B – Voter information in log files

The voting system must prevent the logging of any voter identifying information.

Discussion

The logging and storing of voter identifying information after a ballot is cast violates voter privacy.

Related requirements 10.2.4-C Logging of ballot selections

11.1-C – No disabling logging

The voting system must prevent …

1. the logging capability from being disabled, and
2. the log entries from being modified.

Discussion

- This requirement promotes the integrity of the information logged by ensuring all activities are logged. Additionally, it prevents these abilities from being an option within the user interface.
- This requirement promotes the integrity of the information logged by ensuring all activities are not modifiable.

11.1-D – On-demand access to logs

The voting system must provide administrators access to logs on demand, allowing for continuous monitoring and periodic review.

Discussion

Enabling administrators to export and review the logs is a useful feature. Continuous monitoring and review of access control logs gives the administrator the opportunity to analyze and make changes to permissions and privileges, and quickly identify issues.

Prior VVSG source: 2007 VVSG 4.2.1-A

11.2 - The voting system limits the access of users, groups or roles, and processes to the specific functions and data to which each entity holds authorized access.

11.2.1 – Authorized access

11.2.1-A – Ensuring authorized access

The voting system must allow only authorized users to access the voting system.

Discussion
Authorized users include voters, election officials, and election workers.

11.2.1-B – Modifying authorized user lists

The voting system must allow only an administrator to create or modify the list of authorized users.

Discussion
This requirement assists with ensuring only authorized users are given access to the voting system.

11.2.1-C – Access control by voting stage

The voting system access control mechanisms must distinguish at least the following voting stages from Table 11-1:

1. Pre-voting
2. Activated
3. Suspended
4. Post-voting

Table 11-1 – Voting stage descriptions

Stage	Description
Pre-voting	Powering-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	Occurring when an election official suspends voting
Post-voting	Closing polls, tabulating votes, printing records, powering-off

Discussion
The groups or roles in 11.2-H (Table 2) will be given specific permissions which can be affected by the voting stage (Table 11-1).

Prior VVSG source: VVSG 1.0 I.7.2.1, I.7.2.1.1

11.2.1-D – Access control configuration

The voting system must allow only an administrator to configure the permissions and functionality for each identity, group or role, or process to include account and group or role creation, modification, disablement, and deletion.

Discussion

For vote-capture devices, it is possible for each group or role to have (or not have) permissions for every voting stage. Additionally, the permissions that a group or role has for a voting stage can be restricted to certain functions. Table 3 shows an example matrix of group/role to system 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 or group/role.

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.

The administrator is the only user authorized to make major changes within a voting system. Administrators are given this group or role to ensure all other users have proper access to the information necessary to perform their duties.

11.2.1-E – Administrator modified permissions

The voting system must allow only an administrator to create or modify permissions assigned to specific groups or roles.

Discussion

The administrator's authority to create or modify permissions restricts users from gaining unauthorized permissions.

11.2.1-F – Authorized assigning groups or roles

The voting system must allow only an administrator to create or assign the groups or roles.

Discussion

Table 2 is a list of groups or roles that need to be included within the voting system.

Related requirements: 11.2.2-B – Minimum groups or roles

11.2.2 – Role-based access control

11.2.2-A – Role-based access control standard

Voting systems that implement role-based access control must support the recommendations for Core Role Based Access Control (RBAC) in the ANSI INCITS 359-2004 American National Standard for Information Technology – Role Based Access Control document.

Discussion
This requirement extends [VVSG2005] I. 7.2.1.1-a by requiring role-based methods to follow ANSI INCITS 359-2004.

External references: ANSI INCIS 359-2004
Source: VVSG 1.0 I.7.2.1.1

11.2.2-B – Minimum groups or roles

At minimum, voting systems that implement RBAC must define the following groups or roles within Table 11-2.

Table 11-2 – Minimum Voting System Groups or Roles for RBAC

Group or role	Role description
Administrator	Can update and configure the voting devices and troubleshoots system problems.
Voter	A restricted process in the vote-capture device. It allows the vote-capture device to enter the Activated state for voting activities.
Election Judge	Has the ability to open the polls, close the polls, recover from errors, and generate reports.
Election Worker	Checks in voters and activates the ballot style.
Central Election Official	Loads ballot definition files.

Discussion
Table 11-2 is a baseline list of groups or roles to be included in the voting system.

11.2.2-C – Minimum group or role permissions

At minimum, the voting system must use the groups or roles from Table 11-2 and the voting stages from Table 11-1, to assign the minimum permissions in Table 11-3.

Discussion
Table 11-3 defines the minimum functions according to user, voting stage, and system. Other capabilities can be defined as needed by jurisdiction.

Table 11-3 - Minimum permissions for each group or role

Group/Role	System	Pre-Voting	Activated	Suspended	Post-Voting
Administrator	EMS	Full Access	Full Access	Full Access	Full Access
	BMD/Electronic	Full Access	Full Access	Full Access	Full Access
	PCOS	Full Access	Full Access	Full Access	Full Access
Voter	EMS	---	---	---	---
	BMD/Electronic	---	Vote and cast ballots	---	---
	PCOS	---	Ballot Submission	---	---
Election Judge/Precinct Captain	EMS	---	---	---	---
	BMD/Electronic	Open polls, L&A	Close or suspend polls, Recover from errors	Exit suspended state	Generate reports
	PCOS	Open polls, L&A	Recover from errors	Exit suspended state	Generate reports
Election Worker	EMS	---	---	---	---
	BMD/Electronic	---	Activate ballot and cancel ballots	---	---
	PCOS	---	---	---	---
Central Election Official	EMS	Define and load ballot	---	---	Reconcile provisional-challenged ballots, write-ins, generate reports
	BMD/Electronic	---	---	---	---
	PCOS	---	---	---	---

11.2.2-D – Applying permissions

The voting system must be capable of applying assigned groups or roles and permissions to authorized users.

Discussion

Once the user is assigned a group or role, the voting system needs to be capable of making the necessary changes to the user's permissions. The permissions are changed based on the assigned group or role.

11.3 - The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations.

11.3.1 – Access control mechanism

11.3.1-A – Access control mechanism application

The voting system must use access control mechanisms to permit authorized access or prevent unauthorized access to the voting system.

Discussion

Access controls support the following concepts:

- Limiting the actions of users, groups or roles, and processes to those that are authorized.
- Limiting entities to the functions for which they are authorized.
- Limiting entities to the data for which they are authorized.
- Accountability of actions by identifying and authenticating users.

Most modern operating systems natively provide configurable access control mechanisms that the voting system application can use.

Prior VVSG Source: VVSG 1.1 I.7.2.1.2-1, I.7.2.1.2-2

11.3.1-B – Multi-factor authentication for critical operations

The voting system must be capable of using multi-factor authentication to verify a user has authorized access to perform critical operations, including:

1. Software updates to the certified voting system
2. Aggregation and tabulation
3. Enabling network functions, wireless, and use of telecommunications
4. Changing device states, including opening and closing the polls
5. Deleting or modifying the audit trail
6. Modifying authentication mechanisms

Discussion

NIST SP 800-63-3 Digital Identity Guidelines provides additional information useful in meeting this requirement. NIST SP 800-63-3 defines Multi-factor authentication (MFA) as follows:

"An authentication system that requires more than one distinct authentication factor for successful

authentication. Multi-factor authentication can be performed using a multi-factor authenticator or by a combination of authenticators that provide different factors.
The three authentication factors are something you know, something you have, and something you are.
Multifactor authenticators include, but are not limited to the following:

- Username & password
- Smartcard (for example, voter access card)
- iButton
- Biometric authentication (for example, fingerprint)

External reference: NIST SP 800-63-3 Digital Identity Guidelines

11.3.1-C – Multi-factor authentication for administrators

The voting system must authenticate the administrator with a multi-factor authentication mechanism.

Discussion
This requirement extends [VVSG2005] I.7.2.1.2-e by requiring multi-factor authentication for the voting system administrator group or role.

Prior VVSG source: VVSG 1.1 I.7.2.1.2-e

11.3.2 – Username and password

11.3.2-A – Username and password management

If the voting system uses a user name and password authentication method, the voting system must allow only the administrator to enforce password strength, histories, and expiration.

Discussion
This requirement extends [VVSG2005] I.7.2.1.2-e by requiring strong passwords, password histories, and password expiration.

Prior VVSG source: VVSG 1.1 I.7.2.1.2-1

11.3.2-B – Password complexity

The voting system must allow only the administrator to specify password strength for all accounts including minimum password length, use of capitalized letters, use of numeric characters, and use of non-alphanumeric characters per NIST 800-63 Electronic Authentication Guideline standards.

Discussion

This requirement extends [VVSG2005] I.7.2.1.2-e by allowing the administrator flexibility in configuring password strength. It also requires the use of NIST 800-63 standards.

Prior VVSG source: VVSG 1.1 I.7.2.1.2-1

11.3.2-C – Minimum password complexity

The voting system must compare all passwords against a manufacturer-specified list of well-known weak passwords.

Discussion
Examples of common weak passwords include 0000, 1111, 1234.

Prior VVSG source: VVSG 1.1 I.7.2.1.2-1

11.3.2-D – Usernames within passwords

The voting system must ensure that the username is not used in the password.

Discussion
This requirement extends [VVSG2005] I.7.2.1.2-e by restricting the use of usernames and related information in passwords.

Prior VVSG source: VVSG 1.1 I.7.2.1.2-e

11.4 - Default access control policies enforce the principles of least privilege and separation of duties.

11.4-A – Least privilege for access policies

By default, the voting system must implement the principle of least privilege including denying access to functions and data unless explicitly permitted.

Discussion

This requirement extends [VVSG2005] I.7.2.1.2-a by requiring explicit authorization of subjects based on access control policies.

Prior VVSG source: VVSG 1.1 I.7.2.1.2-1

11.4-B – Separation of duties

Voting system documentation must include suggested practices for dispersing critical operations across multiple groups or roles.

Discussion

Guidance for implementing separation of duties within the voting system is imperative to implement the separation of duties principle. Separation of duties is meant to divide user functions and roles so that there is no conflict of interest.

11.5 - Logical access to voting system assets are revoked when no longer required.

11.5-A – Access time period

The voting system must only allow users authorized access within a time period specified by the administrator.

Discussion
After authentication, a user's access to a voting system will time-out after a specified period of time. This will avoid unauthorized access to the voting system by unauthorized users. Once a user's access has timed-out, the user will have to re-authenticate to continue using the voting system.

11.5-B – Account lockout

The voting system must lockout roles or individuals after an administrator-specified number of consecutive failed authentications attempts.

Discussion
This requirement prevents certain classes of password guessing attacks. This requirement can be implemented using a technique such as exponential backoff. Exponential backoff requires that after each unsuccessful authentication attempt, the time period before another authentication attempt can be made grows exponentially. For instance:

- The wait after 1 unsuccessful authentication attempt is 0 seconds
- The wait after 2 unsuccessful attempts is 2 seconds
- The wait after 3 unsuccessful attempts is 4 seconds, and so on

Prior VVSG source: VVSG 1.1 I.7.2.1.2-1

11.5-C – Lockout time duration

The voting system must allow only an administrator to define the lockout duration.

Discussion
This requirement extends [VVSG2005] I.7.2.1.2 by allowing the administrator flexibility in configuring the account lockout policy. The lockout policy should not lockout voters.

Prior VVSG source: VVSG 1.1 I.7.2.1.2-1