Early Voting Satellite Locations Readiness Checklist Addendum

Secure Connection Requirements

The following NIST 800-53v4 controls must be met for VPN connection:

AC-17 Remote Access

Control Description:

a. The organization establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.

b. The organization authorizes remote access to the information system prior to allowing such connections.

Please reference NIST 800-53v4 Priority 1 High Impact Controls for implementation guidance:

AC-17 (1) (2) (3) (4)

For supporting implementation guidance, please reference NIST 800-53v4 Related Controls:

AC-6, AU-2, AU-12, SC-7, SC-8, SC-12, SC-13

IA-2 Identification and Authentication

Control Description:

a. The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

Please reference NIST 800-53v4 Priority 1 High Impact Controls for implementation guidance:

IA-2 (1) (2) (3) (4) (8) (9) (11) (12)

For supporting implementation guidance, please reference NIST 800-53v4 Related Controls:

AC-6, AU-2, PE-3, SA-4

SC-7 Boundary Protection

Control Description:

a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system.

b. Implements subnetworks for publicly accessible system components that are separated from internal organizational networks.

c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Please reference NIST 800-53v4 Priority 1 High Impact Controls for implementation guidance:

SC-7 (3) (4) (5) (7) (8) (18) (21)

For supporting implementation guidance, please reference NIST 800-53v4 Related Controls:

AC-3, AU-2, CA-9, CP-2, SC-3, SC-8, SC-24

The following NIST 800-53v4 controls must be met for Secure Wireless connection:

AC-18 WIRELESS ACCESS

Control Description:

a. The organization establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and

b. The organization authorizes wireless access to the information system prior to allowing such connections.

Please reference NIST 800-53v4 Priority 1 High Impact Controls for implementation guidance:

AC-18 (1) (4) (5)

For supporting implementation guidance, please reference NIST 800-53v4 Related Controls:

SC-8, SC-13 AC-3, SC-15 PE-19

AC-19 ACCESS CONTROL FOR MOBILE DEVICES

Control Description:

a. The organization establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and

b. The organization authorizes the connection of mobile devices to organizational information systems.

Please reference NIST 800-53v4 Priority 1 High Impact Controls for implementation guidance:

AC-19 (5)

For supporting implementation guidance, please reference NIST 800-53v4 Related Controls:

MP-5, SC-13, SC-28

SI-4 INFORMATION SYSTEM MONITORING

Control Description:

The organization:

a. Monitors the information system to detect:

    i. Attacks and indicators of potential attacks in accordance with HB2178 Minimum Security Standards; and

    ii. Unauthorized local, network, and remote connections.

b. Identifies unauthorized use of the information system through HB2178 approved methods and techniques.

c. Deploys monitoring devices:

    i. Strategically within the information system to collect organization-determined essential information; and

    ii. At ad hoc locations within the system to track specific types of transactions of interest to the organization.

d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.

e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.

g. Provides system monitoring information to Locality IT/Security Manager as applicable.

Please reference NIST 800-53v4 Priority 1 High Impact Controls for implementation guidance:

SI-4 (2) (4) (5)

For supporting implementation guidance please reference NIST 800-53v4 Related Controls:

AU-5, PE-6

CM-6 CONFIGURATION SETTINGS

Control Description:

The organization:

a. Establishes and documents configuration settings for information technology products employed within the information system using HB2178 Minimum Security Checklist that reflect the most restrictive mode consistent with operational requirements.

b. Implements the configuration settings.

c. Identifies, documents, and approves any deviations from established configuration settings for the information system components based on HB2178 operational requirements.

d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

Please reference NIST 800-53v4 Priority 1 High Impact Controls for implementation guidance:

CM-6 (1) (2)

For supporting implementation guidance please reference NIST 800-53v4 Related Controls:

CA-7, CM-4

Chain of Custody Requirements

Items to be included:

1. Voting equipment – transported to early voting locations (seal numbers)
   - Confirmation of seal numbers on all equipment each morning; reseal equipment each evening.
2. Ballots – quantity of each ballot style delivered – confirmation of seals by election staff each morning
   - Seal all blank ballot stock containers each evening and confirm upon opening for business each day of early voting.
3. Voted ballots containers – sealed for delivery back to the Election Office each evening. Confirmation of seals at Election Office upon receipt from early voting locations.

4. Electronic Poll books – transported to early voting locations (seal numbers)
   - Confirmation of seal numbers each morning; reseal equipment each evening; reconfirm seal numbers each morning of early voting.

5. Supply transfer log for all equipment and supplies distributed to each early voting location.
   - Initial by staff along with seal number, if required, on transfer log sheet. At the close of each day of early voting a separate transfer log sheet should be completed, initialed with seal numbers (where required). Election staff team at each early voting location should sign off on the transfer log each morning and each evening.