Mapping to the Handbook for Election Infrastructure Security

Handbook BP #	Handbook Best Practice Title	Essential Guide Best Practice
1	Whitelist which IPs can access the device	
2	Regularly scan the network to ensure only authorized devices are connected	Public-Facing Network Scanning
3	Limit the devices that are on the same subnet to only those devices required	
4	Only utilize approved and managed USB devices with appropriate device encryption and device authentication	• Encrypt Data at Rest • Removable Media
5	Disable wireless peripheral access of devices unless required and the risk is formally approved by election officials	Managing Wireless Networks
6	Ensure the system is segregated from other independent election systems and non- election supporting systems	
7	Deploy Network Intrusion Detection System (IDS) (e.g., MS-ISAC Albert sensor) on internet and extranet DMZ systems	Network Monitoring and Intrusion Detection
8	If wireless is required, ensure all wireless traffic use at least Advanced Encryption Standard (AES) encryption with at least Wi-Fi Protected Access 2 (WPA2)	Encrypt Data in Transit
9	Use trusted certificates for any publicly- facing website	Website Security
10	Ensure logs are securely archived	
11	On a regular basis, review logs to identify anomalies or abnormal events	
12	Ensure critical data are encrypted and digitally signed	• Encrypt Data at Rest • Encrypt Data in Transit
13	Ensure staff is properly trained on cybersecurity and audit procedures and audit every election in accordance with local, state, and federal guidelines	Building and Managing Staff
14	Perform system testing prior to elections (prior to any ballot delivery), such as acceptance testing	
15	Ensure acceptance testing is done when receiving or installing new/updated software or new devices	
16	Conduct criminal background checks for all staff including vendors, consultants, and contractors supporting the election process	Building and Managing Staff
17	Deploy application whitelisting	
18	Work with election system provider to ensure base system components (e.g., OS, database) are hardened based on established industry standards	Managing Vendors
19	Regularly run a SCAP-compliant vulnerability scanner	Public-Facing Network Scanning
20	Utilize EAC certified or equivalent software and hardware products where applicable	Managing Vendors
21	Store secure baseline configuration on hardened offline system and securely deploy baseline configurations	Backups
22	Utilize write once media for transferring critical system files and system updates. Where it is not possible to use write-once media, that media should be used one time (for a single direction off transfer to a single destination device) and securely dispose of the media.	Removable Media
23	Maintain detailed maintenance record of all system components	• Asset Management • Managing Infrastructure
24	Require the use of multi-factor authentication	User Management
25	Require users to use strong passwords (14 character passphrases) if multi factor authentication is not available	User Management
26	Limit the number of individuals with administrative access to the platform and remove default credentials	User Management
27	Ensure that all devices are documented and accounted for throughout their lifecycle	• Asset Management • Managing Infrastructure
28	Utilize tamper evident seals on all external ports that are not required for use and electronically deactivate ports where feasible	Asset Management
29	Maintain an inventory of assets that should be on the same subnet as the election system component	
30	Establish and follow rigorous protocol for installing tamper evident seals and verifying their integrity upon removal	Asset Management
31	Conduct load and stress tests for any transactional related systems to ensure the ability of the system to mitigate potential DDoS type attacks	
32	Limit the use of personally identifiable information. When it is required, ensure that that it is properly secured and staff with access are properly trained on how to handle it.	Endpoint Protection
33	Conduct mock elections prior to major elections to help eliminate gaps in process and legal areas	Exercising Plans
34	Identify and maintain information on network service providers and third-party companies contacts with a role in supporting election activities	Managing Vendors
35	Implement a change freeze prior to peak election periods for major elections	
36	Prior to major elections, conduct in person site audits to verify compliance to security policies and procedures	
37	Work with vendors to establish and follow hardening guidance for their applications	Managing Vendors
38	Ensure logging is enabled on the system	
39	Use automated tools to assist in log management and where possible ensure logs are sent to a remote system	
40	Where feasible, utilize anti-malware software with centralized reporting	Endpoint Protection
41	Ensure only required ports are open on the system through regular port scans	Firewalls and Port Restrictions
42	Where feasible, implement host-based firewalls or port filtering tools	Firewalls and Port Restrictions
43	Verify software updates and the validity of the code base through the use of hashing algorithms and digital signatures where available	Software Updates
44	Ensure vendors distribute software packages and updates using secure protocols	• Managing Remote Connections • Software Updates
45	Maintain a chain of custody for all core devices	Asset Management
46	All remote connection to the system will use secure protocols (TLS, IPSEC)	Managing Remote Connections
47	Users will use unique user IDs	User Management
48	Use a dedicated machine for administrative tasks to separate day to day functions from other security critical functions (For some components this may not be practical to implement)	
49	Ensure that user activity is logged and monitored for abnormal activities	User Management
50	Regularly review all accounts and disable any account that can't be associated with a process or owner	User Management
51	Establish a process for revoking system access immediately upon termination of employee or contractor	User Management
52	Ensure that user credentials are encrypted or hashed on all platforms	User Management
53	Ensure all workstations and user accounts are logged off after a period of inactivity	
54	Ensure your organization has a documented Acceptable Use policy that users are aware of which details the appropriate uses of the system	Building and Managing Staff
55	For data transfers that utilize physical transmission, utilize tamper evident seals on the exterior of the packaging	• Asset Management • Removable Media
56	Disable wireless peripheral access of devices	Managing Wireless Networks
57	Ensure staff is properly trained on cybersecurity and audit procedures and audit every election in accordance with local, state, and federal guidelines	Building and Managing Staff
58	Conduct criminal background checks for all staff including vendors, consultants and contractors supporting the election process	Building and Managing Staff
59	Ensure staff is properly trained for reconciliation procedures for the pollbooks to the voting systems and reconcile every polling place and voter record in accordance with local, state, and federal guidelines	Building and Managing Staff
60	Store secure baseline configuration on hardened offline system and securely deploy baseline configurations	Backups
61	Work with the vendor to deploy application whitelisting	
62	Utilize the most up-to-date and certified version of vendor software	Managing Vendors
63	Utilize write once media for transferring critical system files and system updates. Where it is not possible to use write-once media, that media should be used one time (for a single direction off transfer to a single destination device) and securely dispose of the media.	Removable Media
64	Only use the devices for election related activities	
65	Maintain detailed maintenance records of all system components	• Asset Management • Managing Infrastructure
66	Limit the number of individuals with administrative access to the platform and remove default credentials	User Management
67	Utilize tamper evident seals on all external ports that are not required for use	Asset Management
68	Ensure that all devices are documented and accounted for throughout their lifecycle	• Asset Management • Managing Infrastructure
69	Establish and follow rigorous protocol for installing tamper evident seals and verifying their integrity upon removal	Asset Management
70	Perform system testing prior to elections (prior to any ballot delivery), such as logic and accuracy testing	
71	Ensure acceptance testing is done when receiving or installing new or updated software or new devices	
72	Conduct mock elections prior to major elections to help eliminate gaps in process and legal areas	Exercising Plans
73	Identify and maintain information on network service providers and third-party companies contacts with a role in supporting election activities	• Incident Response • Managing Vendors
74	Implement a change freeze prior to peak election periods for major elections	
75	Prior to major elections, conduct in person site audits to verify compliance to security policies and procedures	
76	Verify software updates and the validity of the code base through the use of hashing algorithms and digital signatures where available	Software Updates
77	Ensure the use of unique user IDs	User Management
78	Ensure individuals are only given access to the devices they need for their job	User Management
79	Maintain a chain of custody for all core devices	Asset Management
80	Ensure all workstations and user accounts are logged off after a period of inactivity	
81	Regularly review all authorized individuals and disable any account that can't be associated with a process or owner	User Management
82	Ensure your organization has a documented Acceptable Use policy that users are aware of which details the appropriate uses of the system	Building and Managing Staff
83	Use secure protocols for all remote connections to the system (TLS, IPSEC)	Managing Remote Connections
84	Ensure critical data is encrypted and digitally signed	• Encrypt Data at Rest • Encrypt Data in Transit
85	Ensure the use of bidirectional authentication to establish trust between the sender and receiver	
86	For data transfers that utilize physical transmission utilize tamper evident seals on the exterior of the packaging	Asset Management
87	Conduct criminal background checks for all staff including vendors, consultants and contractors supporting the election process	Building and Managing Staff
88	Track all hardware assets used for transferring data throughout their lifecycle	• Asset Management • Managing Infrastructure