ELECTION SECURITY BEST PRACTICES GUIDE

TEXAS SECRETARY OF STATE

ELECTIONS DIVISION

www.sos.texas.gov ∗ www.votetexas.gov
1.800.252.8683

(Last Revised: April 2020)

INTRODUCTION

To protect elections throughout the state from **cyber threats**, HB 1421(2019) requires the Texas Secretary of State (SOS) to adopt rules defining classes of protected election data and establishing best practices for identifying and reducing risk to the electronic use, storage and transmission of election data and the security of election systems.

The best practices prescribed in this document were developed by reviewing aggregate findings from the Election Security Assessments (ESAs) of county election offices that were conducted as required by HB 1421, reviewing election security documentation published by the Center for Internet Security and the State and Local Election Security Playbook by Belfer Center, the National Institute for Standards and Technology Cybersecurity Framework, and consultation with select election security experts.

This **Election Security Best Practices Guide** is intended to help Election Authorities, defined as any organization that holds responsibility for conducting elections, by providing guidance on address cyberattack and other disaster risks that the Internet introduces to the election process. Defending elections not only involves protecting voting machines and ballots, but also protecting the functions and technologies that support election processes and manage voter and election result data. While most of the recommendations are directed towards county election offices, these best practices could apply to any entity and individual with a role in conducting elections or managing election-related data before and after elections.

Recognizing that election security must take an all-encompassing, holistic approach, the best practices encompass security issues related to:

- The full election process:
  - Election Process Management
  - Election Staff Support
  - Voter Registration
  - Ballot Creation
  - Voter Check-In
  - Vote Capture
  - Vote Tabulation
  - Election Night Results Reporting
- Physical access to facilities that house election-related technology
- Integrity measures that apply to how staff and volunteers handle information throughout the election process
- Computer workstations and servers
- Devices that access the **network** and Internet such as electronic pollbooks, computers, servers, printers and peripheral devices
- The organization's technology **infrastructure**

It is important to note that these guidelines **do not apply directly to any specific voting machine and tabulation system equipment manufacturer types,** and do not supersede or otherwise replace the various election processes identified in the Texas Election Code, the Texas Administrative Code and Texas Secretary of State Elections Division Advisories.

It is recommended that Election Authorities review this Election Security Best Practices Guide in its entirety with all personnel, Information Technology (IT) teams and other election support teams. The purpose of the review is to determine if current election processes and technology management and use, including items relevant to external vendors and suppliers, follow these cybersecurity best practices. In this way, election authorities can use the guide to identify any security measures that should be put in place.

ORGANIZATION OF ELECTION SECURITY BEST PRACTICES GUIDE

The Election Security Best Practices Guide is broken into two parts. First, we have defined the different classes of election data and provided some general guidelines as to how to develop policies related to securing these data classifications. Second, after defining the classes of election data, we provide the list of best practices. The best practices have been broken into four general categories: **(1) Policy and Processes, (2) Election Processes, (3) Network and IT Infrastructure, and (4) Supporting Technology.**

Within each category, the Election Security Best Practices Guide separates the recommendations into two levels according to their criticality to help Election Authorities prioritize the implementation of the practices: **(1) Priority Best Practices** and **(2) Standard Best Practices**. Priority Best Practices are urgently critical and form the foundation of election cybersecurity. **It is recommended that Election Authorities consider it an imperative priority to implement, at a minimum, the Priority Best Practices.** After achieving the **Priority Best Practices**, election officials should then work on implementing the **Standard Best Practices** which will assist election officials in moving closer to the optimum level of cybersecurity readiness for elections.

This document also includes a summary of the data classifications in **Appendix A** and a prioritized checklist in **Appendix B** that presents the best practices in a summarized format to help Election Authorities track the progress of their election security implementation efforts. Additionally, we've included a glossary in **Appendix C** with definitions of the technical terms used throughout the document.

TEXAS SOS RESOURCES TO HELP IMPROVE ELECTION SECURITY

To assist election officials in adhering to the best practices provided, the Texas SOS has hired election security trainers to provide election officials with individual guidance on how to meet the best practices prescribed. The trainers can also direct election officials to free and low-cost resources that are available to assist with implementing both priority and standard best practices.

Additionally, we have created a **Texas Election Security Toolkit** to help Election Authorities secure their elections. The election security trainers can provide access to the toolkit and can guide election officials in completing the templates in a way that meets their county needs and adheres to prescribed best practices. Including this document, the toolkit consists of a total of six guides:

1. Election Security Best Practices Guide
2. Election Information Security Policy Template
3. Election Incident Response Plan Template
4. Election Continuity of Operations Plan Template
5. Election System Security Plan Template
6. Election Vendor Risk Management Policy Template

Within each guide, we reference the best practices to show which are being addressed when completing different portions of the guides.

The election security trainers are available to work individually with a county or to provide regional trainings on the information contained in the Election Security Toolkit as well as on other general election security topics. To contact our election security trainers or to get access to the Texas Election Security Toolkit, please email electionsecurity@sos.texas.gov with your requests.

Part 1 - DATA CLASSIFICATIONS LEVELS

As Election Authorities develop security policies, plans and processes, data classification levels for voter and election data provide a helpful framework. Data classification ensures that security practices are aligned to the required protections for each data type and how the information is used.

Below you will find four recommended classification levels: **(1) Confidential, (2) Sensitive, (3) Internal Use, and (4) Public Use**. You will notice that there is some overlap between the types of data included in each category. This is intended to give you options depending on how your organization uses and stores the data.

1. **Confidential:** Confidential information is any data that if disclosed could substantially harm the organization and its constituents, impede the conduct of effective government, law and order or violate citizen privacy. This data is likely exempt from disclosure under the provisions of the Texas Public Information Act and other applicable federal and state laws and regulations. It should only be shared with authorized individuals and should be strictly protected with access controls and security measures.
    a. Confidential Data Categories:
        1. Written Information Security Program
        2. Election Information Security Policy
        3. Election System Security Policy
        4. Cybersecurity Incident Response Plan
        5. Continuity of Operations Plan
        6. Vendor Risk Management Policy
        7. Vendor Risk Assessment Results
        8. Election Security Assessment (ESA) Results
        9. Employee and Poll Worker Personally Identifiable Information and Financial Data
        10. Election Department Critical Infrastructure Information
        11. Polling Location Technology Configuration
        12. Passwords, Including Login Credentials for All Systems and Election Devices
        13. Vulnerability Scan Data
        14. Threat Monitoring and Cyber Intelligence Information
        15. System Inventory Information
        16. System Life Cycle Management Information
        17. Security Incident Reports or Event Details
        18. Protected Voter Registration Application Information including items Defined in Election Code 13.004 (c) including:
            a. Social security number
            b. Texas Driver License or TX Personal Identification Card number
            c. Indication that the applicant is interested in working as an election judge
            d. Residence address of federal or state judges and their spouses
            e. Residence address of applicants if the applicant or another person in the applicant’s household is a victim of family violence, sexual assault or abuse, stalking or trafficking
            f. Residence address of applicants participating in the address confidentiality program

g. Residence address of peace officers and other protected individuals under Texas Law.
h. Voter Registration Data Disclosing Criminal History or Voter Activity/Inactivity
i. Voter Registration Application Source Codes

*For the full list and definitions of voter registration data that is confidential, refer to *Texas Election Code § 13.004 Recording and Disclosure of Certain Information by Registrar*

1. **Sensitive:** Sensitive information is data that if altered or deleted could damage the interests of the organization or endanger the safety of citizens. This data can be made publicly available with approval from election official, but it cannot be altered or deleted. It requires a higher than normal assurance of accuracy and completeness. It should be managed with integrity and security measures that ensure accuracy and appropriate availability.
   a. **Sensitive Data Categories:**
      1. Voter Registration Data Excluding Criminal History, Voter Activity/Inactivity and Data Defined as Confidential in Election Code 13.004 (c)
      2. Candidate Application Instructions
      3. Poll Worker Instructions
      4. Election Process Handbook/Guide
      5. Voter Instructions
      6. Candidate Information
      7. Draft Ballot and Proof Information
      8. Preliminary Tabulation Results
      9. Vendor Information Excluding Vendor Risk Assessment Results
      10. Password Management Policies
      11. Technology Storage and Transportation Details
      12. Escalation Path and Communication Plans for Suspected Security Incidents or Events
      13. Roles and Responsibility Definitions and Assignments

2. **Internal Use**: Internal Use information is data that is intended only for use within the Election Department. External access to this data should be prevented but disclosures are not critical. Internal access should be limited to only those individuals who require the data to perform their job duties. Data in this category may become available to the public, if a public information request or inquiry is received and approved.
   a. **Internal Use Data Categories:**
      1. Employee Handbooks
      2. Security Awareness Training
      3. Pollbook Technology Details
      4. Background Check Processes
      5. Vendor Information
      6. Chain of Custody Documentation for Voting Systems and Ballots
      7. Help Desk Instructions
      8. Basic Facts About a Security Incident or Event
         a. It Happened
         b. It Is Being Addressed Rapidly
         c. How It Impacts Voters

2. **Public Use**: Public Use information is non-sensitive data that if distributed outside of the Election Department will not adversely impact the organization or citizens. This data has been declared public knowledge by someone with the proper authorization and should not be used or disclosed without approval.
    a. **Public Use Data Categories**
        1. Election News and Announcements
        2. Job Announcements
        3. Election System and Voting Equipment Types
        4. Voting System Type
        5. Poll Locations
        6. Election Schedules
        7. Ballot Information
        8. Tabulation Results
        9. Official Domain URLs

Part 2 - ELECTION SECURITY BEST PRACTICES

Category 1: POLICIES AND PROCESS

1. **CREATE AN AUTHORIZED ELECTION WRITTEN INFORMATION SECURITY PROGRAM (WISP).** A WISP is a set of policies and plans that define how to protect elections from cyberattack and how to respond if an incident occurs. It authorizes employees to quickly perform the described actions without waiting for approval during an attack.

   a. Ensure that all policies and plans are authorized by the appropriate authorities and are officially adopted and implemented by the staff and IT teams.

   b. Review the plans and policies in the WISP at least once a year according to the following schedule:

      i. During general election years, in December after an election to incorporate any needed improvements and clarification identified during the election as well as new risks

      ii. During legislative session years, in July after the state election law conference to incorporate any new laws affecting elections as well as new risks

   PRIORITY BEST PRACTICES

   c. Create an **Election Information Security Policy.** The purpose of an Election Information Security Policy is to establish protocols that protect election-related data from cyber threats and other disasters.

      i. Develop a data classification system that can be used to establish the appropriate security needed for each data type. See Data Classifications in Part 1 for more guidance.

      ii. Organize the policy around the five security objectives established by the **National Institute of Standards and Technology (NIST)** Cybersecurity Framework (CSF): (1) Identify (2) Protect (3) Defend (4) Respond, and (5) Recover.

   d. Create an **Incident Response Plan** that documents the specific steps to take in case of cyberattack or other types of disasters.

      iii. An Incident Response Plan should include:

         1. A clear definition of what constitutes a cyberattack or incident
         2. A classification system for the severity level of incident types and the appropriate notification and response protocol for each type
         3. **Incident containment processes** that minimize the scale and scope of the damage
         4. Procedures for restoring systems and operations after an attack

      iv. An incident Response Plan should address, at a minimum, the following incidents:

         1. Malware
         2. **Ransomware**
         3. **Denial of Service (DoS) and Distributed Denial of Services (DDoS)**
         4. Intrusion
         5. Information access
         6. Compromised data

7. Insider threats
8. Compromised accounts
9. Loss or theft of election and/or computer systems
10. Social engineering attack
11. Data breach

e. Create a **Continuity of Operations Plan** (**COOP).** A COOP should consider how a cyberattack may disrupt an election and explain fail-safes, backup processes and systems to keep critical functions operating if a cyber incident occurs.

   i. Align the COOP with the Incident Response Plan for consistency and clarity.

STANDARD BEST PRACTICES

f. Create an **Election System Security Plan**. An election system security plan provides written protocols that protect election-related equipment housing election data from cyber threats and other disasters. An Election System Security Plan should:

   i. Describe job functions and the responsibilities of the roles that interact with each system.
   ii. Define security controls that encompass the full scope of how election and IT systems support elections.
   iii. Include the complete range of election processes from registering voters to reporting results.
   iv. Identify how systems work together to accomplish each election function.
   v. Outline how election equipment and systems are secured and stored.
   vi. Include how voters interact with systems

g. Create a **Vendor Risk Management Policy.** A Vendor Risk Management Policy is a written policy that creates guidelines for an election office to ensure that third-party vendors are not introducing security gaps that bad actors can exploit to stage an attack. As part of the policy, election offices should request that their vendors:

   i. Provide a copy of their Information Security Policies and Plans to determine whether the vendor practices reasonable security measures.
   ii. Allow periodic evaluation and information gathering on how they protect information and systems.
   iii. Have documented controls or procedures on how they secure USB devices and any associated removable media.
   iv. Document how the vendor will support the organization during execution of the Continuity of Operations Plan.

2. MONITOR CONTINUOUSLY FOR THREATS

PRIORITY BEST PRACTICES

a. Contract an external security service provider to monitor the network and remote systems 24 hours every day and analyze events for indicators of cyberattack. Available services include:

   i. Albert Sensor from the Center for Internet Security (CIS)
   ii. Monitoring services available through the Texas Department of Information Resources (DIR)

b. Ensure the service provider uses effective threat monitoring software and hardware products, particularly a **Security Incident and Event Management (SIEM)** solution.

3. PERFORM VULNERABILITY SCANNING AND PATCH MANAGEMENT

PRIORITY BEST PRACTICES

a. Establish a monthly **patch management** process to address any operating system and software application vulnerabilities.

b. Conduct monthly **vulnerability scans** of all internal systems and maintain a log of recent scans. The log should include:

   i. Details about detected vulnerabilities

   ii. Records of any remediation steps taken to fix the vulnerability

4. CLASSIFY AND PROTECT ELECTIONS DATA

PRIORITY BEST PRACTICES

a. Review and Identify Confidential, Sensitive and Internal Use Data within the Elections environment as described in the Data Classification Guidelines.

b. Ensure that all Confidential, Sensitive and Internal Use data has these best practices applied appropriately, such as implementing encryption for Confidential Data and limit access to systems to only approved and authorized users.

c. Control which users have access to each class of elections data, through process and technology, where possible. Evaluate the roles of the staff and consider limitations such as:

   i. Confidential Data should be limited to the Election Authority and a very limited support team that requires access as necessary to conduct their job duties.

   ii. Sensitive Data should be limited to employees and Full-Time Elections staff.

   iii. Temporary election staff access should be limited to subsets of information where possible and have an account assigned to them individually so that access to data can be monitored.

4. PARTICIPATE IN SECURITY AWARENESS TRAINING

PRIORITY BEST PRACTICES

a. Each member of the election department staff is required to participate in the SOS cybersecurity training required by and provided by the Texas SOS Office.

b. Each staff member is required to repeat the security training annually

c. Election officials should discuss the security recommendations in the training videos with staff to create a culture of security awareness.

6. CONDUCT ELECTION SECURITY ASSESSMENTS REGULARLY

PRIORITY BEST PRACTICES

a. Participate in the Election Security Assessment provided by the Texas SOS Office as required by Section 279.003, Texas Election Code.

b. Conduct subsequent security assessments at least once every two to four years or more often if the political subdivision has a significant change in structure or circumstance such as purchasing new equipment, moving to a new office, or changing personnel. Certain political subdivisions may be eligible for assessments provided by DHS. Election authorities may also contract with private entities to conduct security assessments.

c. Use the ESA results and the results from any subsequent assessment to establish a roadmap defining how and when the required improvements will be made.

STANDARD BEST PRACTICES

d. Review the most recent ESA every year to ensure recommendations were effectively implemented, identify opportunities for improvement and maintain alignment with the roadmap.

e. Use the vendor risk management review included in the ESA to develop requirements for the Vendor Risk Management Policy.

7. PARTICIPATE IN THE DHS MS-ISAC AND EI-ISAC INFO SHARING PROGRAM

a. Election Officials should join the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) information services and IT officials should join the Multi-State Information Sharing and Analysis Center (MS-ISAC) and provided by the Department of Homeland Security (DHS).

b. Review communications and develop a process for monitoring the cyber threats tracked and reported by the MS-ISAC/EI-ISAC Security Operations Center (SOC)

Category 2 - ELECTION PROCESS

1. IMPLEMENT A TWO PERSON VERIFICATION PROCESS

PRIORITY BEST PRACTICES

a. Ensure that every election function from ballot programming to Election Night Reporting uses a two-person verification method in which one person performs the task and a second person witnesses and verifies the accuracy and integrity of the result.

b. Two-person verification should occur during:

   i. Ballot programming of electronic and paper ballots

   ii. Election device programming

   iii. Receipt of election media devices

   iv. Breaking and attaching tamper-evident seals

   v. Ballot counting

   vi. Tabulation of election results

   vii. Election Night Reporting of results

c. In accordance with the state election code information retention policy, keep a record with full signatures from the two people who participated in the verification process.

d. Work closely with election vendors to foster an environment of two-person verification.

2. ELECTION NIGHT REPORTING INTEGRITY

PRIORITY BEST PRACTICES

a. Only disseminate results to the public on election night through the organization's official website.

   i. Use email messages and social media posts to direct the public to the official website to view the election results.

   ii. Do not email results to certain parties or the media, and do not publish results through social media accounts.

STANDARD BEST PRACTICES

b. Include the following integrity validation measures on the website when publishing results:

   i. The organization's logo or seal on the document or a watermark in the document header or footer.

   ii. A file **checksum** value that can verify legitimate results. A free Microsoft utility can accomplish this. (https://support.microsoft.com/en-us/help/841290/availability-and-description-of-the-file-checksum-integrity-verifier-u)

iii. A statement that the results are unofficial until after the election canvass and post of the date of the canvass.

c. Remove previous unofficial results from the website once the official results are completed or move to a section of your website titled “historical results.”

d. Do not post unofficial or official reports printed from tabulation systems or results pages that include the election system vendor’s name.

3. DOCUMENT ELECTION PROCESSES

STANDARD BEST PRACTICES

a. Create an election handbook that captures the experience and expertise of key staff members to clearly outline the full scope of the election process.

b. Ensure that the handbook accomplishes key election department objectives such as:

i. Facilitating cross training between roles and departments

ii. Enabling the consistent implementation among staff members of election security best practices

iii. Understanding and following the Written Information Security Program’s plans and policies

4. PHYSICALLY SECURE ELECTION OFFICES AND SYSTEMS

PRIORITY BEST PRACTICES

a. Establish a chain of custody documentation process for election systems that includes:

i. The original source of the system

ii. When the system first arrived at the organization

iii. Who received the system

iv. Condition of the system

v. Where the system is stored

vi. When the election system is used in a different location, such as a polling site, document:

- Date
- Time
- Who issued the system
- Who received and transported the system
- The location where it was used

vii. When the system is returned to its storage location, document:

- Date
- Time
- Who transported and returned the system
- Who received the system
- Storage location

b. Never leave systems with network access unattended unless they are in a locked area.

c. Control physical access to election equipment at all times and utilize tamper evident seals for integrity protections, even when they are not in use for elections.

d. Set up a secure perimeter with functioning conventional or digital locks protecting all entry points.

e. Use trackable access codes or keycards if possible, or at minimum implement entry and exit logs to track entry to secure areas where election systems are located.

f. Identify all visitors to your election office

   i. Visitors should enter and exit in a controlled area.

   ii. Document time of arrival.

   iii. Provide visitor credentials to be displayed while in the secure area.

   iv. Require an escort by a member of the election staff at all times.

   v. Document the time of departure.

g. Use an access control key or password witnessed by one or more individuals when securing election equipment. Document the use of an access control key in a log dedicated for that purpose and have a witness sign the log.

h. Monitor all entry and exist points to election facilities with cameras that have recording capability and have security personnel patrol the area when possible. Review the camera footage if an incident occurs.

i. Adhering to the state election code information retention policy time requirements, keep all chain of custody documentation, camera footage and access logs documenting secure area entry/exit and access control key or password use.

Category 3 - NETWORK AND INFRASTRUCTURE

1. INSTALL A NEXT GENERATION FIREWALL

PRIORITY BEST PRACTICES

a. Install an **enterprise-class**, **next generation firewall (NGFW)** to segment election systems, functions and data from the rest of the network and strengthen Internet security. The next-generation firewall should include:

- **Network Segmentation** Capabilities
- **Stateful Deep Packet Inspection**
- **Virtual Private Network (VPN)** Support
- Web-traffic Filtering
- Intrusion Detection and Prevention System
- Application Inspection and Control
- Geolocation Blocking
- DoS, DDoS, and **Port Scan Blocking**

b. Configure the firewall to control outbound activity from election computers and to block unauthorized access to the network from the Internet or other network segments and networks that support the organization.

c. Check for firewall patches and updates on a monthly basis in alignment with the Vulnerability Scanning and Patch Management best practice.

2. SEGMENT THE NETWORK

PRIORITY BEST PRACTICES

a. Using a firewall or Next Generation Firewall, partition the network to create a section dedicated to election-related functions.

b. Protect access to this segment from the rest of the network, other networks or the Internet with its own firewall (see additional guidance on firewall implementation in the Network and Infrastructure section.)

c. Restrict access to the election segment of the network to only employees who need the data it contains to perform their job duties.

3. UPGRADE UNSUPPORTED END-OF-LIFE OPERATING SYSTEMS AND SOFTWARE.

PRIORITY BEST PRACTICES

a. Upgrade or replace operating systems earlier than Windows 10 Professional or Windows 10 Enterprise.

b. Ensure that the software installed on systems used to support elections is current and critical security patches are up to date.

c. Check for patches and updates on a monthly basis in alignment with the Vulnerability Scanning and Patch Management best practice.

4. RESTRICT NETWORK ACCESS

PRIORITY BEST PRACTICES

a. Limit remote access to the election network.

b. Tightly control management tools that grant remote access to a limited number of employees.

c. Permit only vendor connections that have been evaluated according to the Vendor Risk Management Policy.

d. Prohibit network access through internet access points or other connections that are not protected by the next-generation firewall.

5. USE ENDPOINT SECURITY SOLUTIONS

PRIORITY BEST PRACTICES

a. Prevent **endpoints** from enabling attackers to access the network by implementing Endpoint Security Solutions that detect and block threats. The solution should include:

  i. Anti-virus/Anti-malware

  ii. Ransomware protection

  iii. Host Intrusion Detection System (HIDS)

b. Deploy the solution on all endpoint devices, except systems provided for vote tabulation.

c. Check for patches and updates on a monthly basis in alignment with the Vulnerability Scanning and Patch Management best practice.

6. IMPLEMENT SOFTWARE AND NETWORK WHITELISTING

PRIORITY BEST PRACTICES

a. Configure each election system with software such as Endpoint Security Software or Windows 10 Enterprise that prohibits the execution of unapproved software packages including: Applications, Email, **Web Servers,** and Endpoint Devices.

b. Establish a process that requires approval for additional software package installations.

c. Protect access to the election network by preventing any unapproved devices from communicating with systems behind the firewall.

d. Disable unused **network ports** at the **network switch**.

e. Configure active ports to block access to unapproved devices and prevent unauthorized network access.

7. SECURE WIRELESS NETWORKS AND DEVICES

PRIORITY BEST PRACTICES

a. Disable or deactivate wireless devices (Wi-Fi and Bluetooth) that are not in use or defined in the acceptable use policy.

b. Separate (**network segmentation**) all other Wi-Fi networks from the election department’s Wi-Fi network

STANDARD BEST PRACTICES

c. Create a policy that defines acceptable use of wireless devices.

d. Configure Wi-Fi networks to use **Wi-Fi Protected Access 2 (WPA2)** or later security controls that adhere to the Advanced Encryption Standard (AES).

e. Ensure that passphrases meet the minimum password standards.

f. Hide the election department's **Service Set Identifier (SSID).**

g. If Wi-Fi is used to support a polling place, restrict the wireless network to supporting only the required ePollbook functionality.

8. BACKUP DATA OFFSITE USING ENCRYPTION

PRIORITY BEST PRACTICES

a. Backup critical election data daily on encrypted backup drives or systems housed offsite. When using a computer system as backup, ensure that the system is not connected to the election network.

b. Backup all data that can be classified as Confidential, Sensitive or Internal Use (defined above) related to election activities.

c. Encrypt and store backup data using **FIPS 140-2 encryption** levels.

9. ENCRYPT ELECTION AND VOTER INFORMATION

PRIORITY BEST PRACTICES

a. Encrypt data storage for servers that support the election environment. All data that is classified as Confidential, Sensitive or Internal Use (as defined above) must be stored in an encrypted file system or system disk.

b. Require encryption for cloud solutions used to store Confidential, Sensitive or Internal Use information (such as voter registration applications or election management information).

STANDARD PRACTICES

c. Encrypt the hard disks of computer systems that access and process voter registration information or critical election data using an encryption product such as Windows BitLocker.

10. MANAGE REMOVABLE MEDIA USE

PRIORITY BEST PRACTICES

a. Create a **Removable Media** Policy as part of the Election Information Security Policy defining a list of approved media and their uses. Removable media includes USBs, Thumb drives, Memory sticks, Data cards and CDs.

b. For general purpose removable media use, allow only encrypted USB devices

c. Assign removable media device management to a single person

d. Keep a log to track removable media assignments and regulate their use at all times.

STANDARD BEST PRACTICES

e. Use software such as Endpoint Security Software or Windows 10 Enterprise that controls the use of specific removable media devices.

f. Supply and certify removable media devices such as USB keys or drives used by staff and ensure their use adheres to the Removable Media Policy.

g. Put removable media devices that transfer information between non-connected election systems through a USB cleaning process that deletes the contents on the device before they are stored or reused. Consider implementing a single-use policy for devices used to transfer data between non-connected systems where possible.

h. Delete contents and securely destroy single use removable media, such as write once DVDs (DVD-R), CDs (CD-R), and USB drives.

11. TRACK INVENTORY

PRIORITY BEST PRACTICES

a. Create a detailed inventory list of all technology used to support and conduct an election.

b. Maintain a digital and/or paper log of approved software and removable media devices that includes identifying features such as:
    i. Model
    ii. Serial number
    iii. Unique asset tag number
    iv. Location of deployment
    v. Person who issued the equipment
    vi. Person receiving returned equipment
    vii. Location of stored equipment

STANDARD BEST PRACTICES

c. Identify devices used for an election, including the identification of devices used during early voting separately from those used for Election Day and retained between elections.

d. When reusing a device, include a description of its contents before erasing the information and using the device again.

e. Keep inventory records for the amount of time specified in the applicable information retention policy.

Category 4 - SUPPORTING TECHNOLOGY

1. CONTROL AND PROTECT EMAIL AND WEBSITE DOMAINS

PRIORITY BEST PRACTICES

a. Election staff members should only use government-provided email addresses or web servers.

b. Counties should utilize official government domains ending in texas.gov or tx.us. Contact the Texas Department of Information Resources (DIR) for assistance in obtaining a texas.gov address.

c. Never perform election business from a non-government email address or website.

d. Implement a **Web Application Firewall (WAF)** for additional website security.

e. Update election website software with critical patches once per month.

STANDARD BEST PRACTICES

f. Perform a penetration test once a year for websites that provide election results or voter or election information

g. Ensure that all transmissions over election websites use a **Secure Socket Layer (SSL)** certificate that provides users with privacy and ensures that they are on the official website.

2. IMPLEMENT EMAIL SECURITY

PRIORITY BEST PRACTICES

a. Disable web-based internet access to email or require that Multi-Factor Authentication be used for web-based email access.

b. Integrate into your email system **Domain-Based Message Authentication, Reporting and Conformance (DMARC),** an email service that helps to identify legitimate email sources to prevent email spoofing, into your existing inbound email authentication process.

STANDARD BEST PRACTICES

c. Use multifactor authentication to control access to all email accounts

d. Implement SPAM filtering measures in the email server at the point of initial mail receipt.

e. Include anti-virus scanning of email messages to detect and block message attachments that contain viruses.

3. PASSWORDS AND MULTI-FACTOR AUTHENTICATION (MFA)

PRIORITY BEST PRACTICES

a. Require that every system used for election functions has a unique username for each individual staff member that is authorized to access the system.

b. Do not allow shared user accounts.

c. Use a Password Management Solution that stores passwords in an encrypted format and includes multifactor authentication to access.

d. Never write passwords down or keep them in locations that are accessible to others.

e. Never store passwords in spreadsheets, journals, or email contacts applications.

f. Update password policies on all systems to support the following complex password requirements:
   i. At least 12 characters
   ii. At least 1 upper case letter
   iii. At least 1 lower case letter
   iv. At least 1 number
   v. At least 1 special character

g. Force updates every 90 days

h. Enable multifactor authentication on Domain Administrator accounts.

i. Ensure that any system accessed remotely to support election processes uses multifactor authentication, including any election service provider portal or secure file transfer system.

STANDARD BEST PRACTICES

j. Implement Multi-Factor Authentication for all systems, internal and external, that support the election network or office.

k. Implement MFA solutions using soft tokens such as Microsoft Authenticator or Duo for the additional authenticating factor instead of text or email.

l. Discourage staff from sharing passwords or using joint accounts to any systems. If using a joint account is required, outline processes that detail security protocols to limit use.

m. Change system default passwords immediately after initial setup of a new system or device.

4. LIMIT ADMINISTRATOR ACCESS

PRIORITY BEST PRACTICES

a. Limit unauthorized access to endpoint computers and devices by configuring the Local Administrator account default settings during initial setup on all systems:
   i. Immediately change the default Local Administrator account password to a unique complex password.
   ii. Disable access to the Local Administrator account from the network.

b. Limit access to Domain Administrator accounts to authorized personnel only (typically the IT department) and require Multi-Factor Authentication for Domain Administrator accounts.

c. Establish a user hierarchy based on the **Principle of Least Privilege** to ensure that users don’t have more access to administrative capabilities than they need to perform their job duties.

d. Establish an approval process for users who require **system or application administrator access** privileges, and never assign an administrative account to a user who does not require administrator-level control.

e. Ensure that administrators use a user account with end-user level permissions for routine operations and a separate administrator account for privileged administrative tasks.

APPENDIX A: DATA CLASSIFICATION CHART

TABLE 2: ELECTION DATA CLASSIFICATION SYSTEM	
Confidential information is any data that if disclosed could substantially harm the organization and its constituents, impede the conduct of effective government, law and order or violate citizen privacy. This data is exempt from disclosure under the provisions of the Texas Public Information Act and other applicable federal and state laws and regulations. It should only be shared with authorized individuals and should be strictly protected with access controls and security measures.	• Written Information Security Program • Election Information Security Policy • Election System Security Plan • Cybersecurity Incident Response Plan • Continuity of Operations Plan • Vendor Risk Management Policy • Vendor Risk Assessment Results • Election Security Assessment (ESA) Results • Employee and Poll Worker Personally Identifiable Information and Financial Data • Election Department Critical Infrastructure Information • Polling Location Technology Configuration • Passwords, Including Login Credentials for All Systems and Election Devices • Vulnerability Scan Data • Threat Monitoring and Cyber Intelligence Information • System Inventory Information • System Life Cycle Management Information • Security Incident Reports or Event Details • Protected Voter Registration Application Information including items Defined in Election Code 13.004 (c) including: o Social security number o Texas Driver License or TX Personal Identification Card Number o Indication that the applicant is interested in working as an election judge o Residence address of federal or state judges and their spouses o Residence address of applicants if the applicant or another person in the applicant's household is a victim of family violence,

	sexual assault or abuse, stalking or trafficking o Residence address of applicants participating in the address confidentiality program o Residence address of peace officers and other protected individuals under Texas Law. o Voter Registration Data Disclosing Criminal History or Voter Activity/Inactivity o Voter Registration Application Source Codes *For the full list and definitions of voter registration data that is confidential, refer to *Texas Election Code § 13.004 Recording and Disclosure of Certain Information by Registrar*
Sensitive	
Sensitive information is data that if altered or deleted could damage the interests of the organization or endanger the safety of citizens. This data can be made publicly available with approval, but it cannot be altered or deleted. It requires a higher than normal assurance of accuracy and completeness. It should be managed with integrity and security measures that ensure accuracy and appropriate availability.	• Voter Registration Data Excluding Criminal History, Voter Activity/Inactivity and Data Defined as Confidential in Election Code 13.004 (c) • Candidate Application Instructions • Poll Worker Instructions • Election Process Handbook/Guide • Voter Instructions • Candidate Information • Draft Ballot and Proof Information • Preliminary Tabulation Results • Vendor Information Excluding Vendor Risk Assessment Results • Password Management Policies • Technology Storage and Transportation Details • Escalation Path and Communication Plans for Suspected Security Incidents or Events • Roles and Responsibility Definitions and Assignments
Internal Use	
Internal Use information is data that is intended only for use within the Election Department. External access to this data should be prevented but disclosures are not critical. Internal access should be limited to only those individuals who require the data to perform their	• Employee Handbooks • Security Awareness Training • Pollbook Technology Details • Background Check Processes • Vendor Information • Chain of Custody Documentation for Voting Systems and Ballots • Help Desk Instructions • Basic Facts About a Security Incident or Event

job duties. Data in this category may become available to the public, if a public information request or inquiry is received and approved.	○ It Happened ○ It Is Being Addressed Rapidly ○ How It Impacts Voters
Public Use	
Public Use information is non-sensitive data that if distributed outside of the Election Department will not adversely impact the organization or citizens. This data has been declared public knowledge by someone with the proper authorization and should not be used or disclosed without approval.	• Election News and Announcements • Job Announcements • Election System and Voting Equipment Types • Voting System Type • Poll Locations • Election Schedules • Ballot Information • Tabulation Results • Official Domain URLs

APPENDIX B: BEST PRACTICE CHECKLIST

ELECTION SECURITY BEST PRACTICES CHECKLIST		
	❒ Ensure policies and plans are authorized ❒ Review yearly by appropriate personnel ❒ Create Election Information Security Policy ❒ Create Incident Response Plan ❒ Create Continuity of Operations Plan	❒ Create Election System Security Plan ❒ Create Vendor Risk Management Policy
	❒ Establish 24/7 security monitoring services ❒ Ensure provider uses effective products including a SIEM.	
	❒ Establish a monthly patch management process ❒ Conduct monthly vulnerability scans	
	❒ Assign election data to data classification categories ❒ Apply appropriate protections for each data classification category ❒ Give users access to only the least amount of data needed for their role	
	❒ Each member of the election staff is required to participate in the SOS cybersecurity training ❒ Repeat security training every year ❒ Discuss security recommendations with staff	
	❒ Participate in the ESAs provided by Texas SOS	❒ Use ESA results to establish an improvement roadmap ❒ Review ESA results yearly

	❒ Conduct follow-up assessments at least once every two to four years (or more often if necessary)	
	❒ Become a member of the MS-ISAC/EI-ISAC ❒ Develop a process for monitoring the cyber threat reports	
	❒ Ensure that one person performs the task and a second person witnesses and verifies result integrity for every election function ❒ Keep a record with full signatures from both people ❒ Encourage election vendors to implement two-person verification ❒	❒ Use integrity validation measures on the website when publishing results ❒ Do not post unofficial or official reports printed from tabulation systems or that include the election vendors name
	❒ Only disseminate results to the public on election night through the official website ❒ Do not email results to external parties or the media ❒ Do not publish results through social media accounts Use email and social media to direct the public to the official website to view election results	
		❒ Create an election handbook that captures the experience of key staff members ❒ Ensure the handbook accomplishes key election department objectives
	❒ Establish a chain of custody documentation process for election systems ❒ Never leave a systems network with access unattended unless they are in a locked area	

	❒ Control physical access to election equipment at all times ❒ Use tamper evident seals on election equipment, even when they are not in use for elections ❒ Use functioning conventional or digital lock to protect all entry points to election facilities ❒ When locking up election equipment, use an access control key or password, have one or more person as a witness and sign a log verifying the equipment is secure ❒ Monitor entry and exist points to election facilities with cameras that have recording capability ❒ Adhere to the information retention policy time requirements for keeping logs, documentation and camera footage	
NETWORK AND INFRASTRUCTURE		
Install a Next-Generation Firewall	❒ Configure the firewall to control outbound activity and block unauthorized access ❒ Check for patches and updates monthly	
Segment the Network	❒ Use the firewall to create a network section dedicated to election functions and data ❒ Protect access from the rest of the network, other networks and the Internet ❒ Restrict access to the election segment of the network to only election employees	
Update Unsupported Operations Systems and Software	❒ Upgrade or replace operating systems earlier than Windows 10 Professional or Windows 10 Enterprise	

	❒ Ensure all election-related software is current and security patches are up to date ❒ Check for patches and updates monthly	
Restrict Remote Network Access	❒ Limit remote access to the election network ❒ Tightly control remote access tools and limit use to select employees. ❒ Vendors must meet the terms of the Vendor Risk Management Policy before connecting to the network ❒ Prohibit network access through Internet access points not protected by the firewall	
Use Endpoint Security Solutions	❒ Ensure Endpoint Security Solutions detect and block threats ❒ Deploy on all endpoint devices, except systems provided for vote tabulation ❒ Check for patches and updates monthly	
Implement Software and Network Whitelisting	❒ Configure election systems with software that prohibits unapproved software packages ❒ Establish an approval process for software installation ❒ Prevent unapproved devices from communicating with systems behind the firewall ❒ Disable unused network ports at the network switch Ensure active ports block access to unapproved devices	
Secure Wireless Networks and Devices	❒ Disable Wi-Fi and Bluetooth wireless devices that are not in use or not defined in the acceptable use policy	❒ Create a policy that defines the acceptable use of wireless devices ❒ Configure Wi-Fi networks to use WPA2 or later security controls

	❒ Segment the network to separate all other Wi-Fi networks from the election department’s Wi-Fi network	❒ Ensure passphrases meet minimum password standards ❒ Hide the election department SSID ❒ Restrict polling location wireless networks to required ePollbook functionality only
Backup Data Offsite Using Encryption	❒ Backup daily to an encrypted system offsite and not connected to the election network ❒ Backup all data related to election activities ❒ Encrypt and store data at FIPS 140-2 encryption levels	
Encrypt Election and Voter Information	❒ Encrypt data storage for servers that support elections ❒ Require encryption for cloud solutions used to store voter registration and critical election information	❒ Encrypt hard disks of computer systems that access and process voter registration and critical election data
Manage Removable Media Use	❒ Create a Removable Media Policy as required in the Election Information Security Policy template ❒ Allow only encrypted USB devices for general purpose removable media ❒ Assign management of election-related removable media devices to one person ❒ Track removable media assignments in a log and regulate use at all times	❒ Use software that controls the use of removable media devices ❒ Put removable media devices that transfer information between non-connected elections systems through a USB cleaning process ❒ Delete contents and securely destroy single-use removable media
Track Inventory	❒ Create a detailed inventory list of all technology used to support and conduct an election ❒ Maintain a digital or paper log of approved software and removable media	❒ Divide the inventory list into three separate sections: early voting, election day and between elections ❒ When reusing a device, add a description of device contents to the inventory list before erasing the information

		□ Keep inventory records for the time specified in the information retention policy.
SUPPORTING TECHNOLOGY		
Protect Email and Website Domains	□ Only use government-provided email addresses and web services using the Internet domain texas.gov or tx.us □ Never perform election business from a non-government email address or website □ Update election website software with critical patches once per month □ Perform penetration tests once per year on election websites	□ Ensure all election website transmissions use a SSL certificate □ Implement a Web Application Firewall
Implement Email Security	□ Disable or require multi-factor authentication for web-based Internet access to email □ Integrate DMARC into your email system	□ Use multifactor authentication to control access all email accounts □ Implement SPAM filtering □ Use anti-virus scanning tools
Password and Multifactor Authentication (MFA)	□ Assign unique usernames to staff members authorized to access any system used for election functions □ Do not allow shared user accounts □ Use a password management solution that uses an encrypted format and requires MFA □ Configure password policies on all systems to require complex passwords □ Require MFA for Domain Administrator access □ Ensure any system accessed remotely to support election processes uses MFA	□ Use MFA on all systems whenever possible □ Use soft tokens as the second user identifying factor instead of text or email □ Discourage staff from sharing passwords or joint accounts □ Change system default passwords immediately after initial new system or device setup
Limit Administrator Access	□ Add constraints for the Local Administrator Account	□ Establish a user hierarchy based on the Principle of Least Privilege

	❒ Limit access to Domain Administrator accounts to authorized personnel only	❒ Implement an approval process for administrator access ❒ Ensure that administrators use a user account for routing operations separate from the administrator account used for administrative tasks

APPENDIX C: GLOSSARY

CHECKSUM	A technique used to verify that a file is not corrupted by a virus or other code by using a unique digital fingerprint of the data.
CONTINUITY OF OPERATIONS PLAN	Procedures that enable the election department to continue to operate with minimal disruption during a cyberattack or other disaster.
CYBER THREATS	Criminal activity seeking to undermine elections or steal data for financial gain using the Internet to disrupt or infiltrate election technology
CYBERSECURITY RISKS	Gaps in security practices that present opportunities for cyber criminals to successfully attack election departments.
DENIAL OF SERVICE (DoS)	An attack in which the cybercriminal blocks user access to a computer network.
DOMAIN-BASED MESSAGE AUTHENTICATION REPORTING AND CONFORMANCE (DMARC)	An email validation protocol that protects email domains from unauthorized use.
ELECTION INFORMATION SECURITY POLICY	Protocols that protect election-related data from cyber threats and other disasters.
ELECTION SECURITY ASSESSMENT (ESA)	Cybersecurity reviews to determine the security status of election departments and identify areas for improvement.
ELECTION SYSTEM SECURITY PLAN	Protocols that protect election systems from cyber threats or other disasters.
END-OF-LIFE	The point at which a computer, system, or software should be retired because it can no longer function at optimal levels due to wear, outdated technology, and lack of manufacturer support.
ENDPOINTS	User devices such as computers, laptops, tablets, and printers that are connected to the network.
ENTERPRISE-CLASS SYSTEM	A system with advanced capabilities and large capacity to handle high volume and complex demands.
FEDERAL INFORMATION PROCESSING STANDARD (FIPS) 140-2	A U.S. government computer security standard used to approve cryptographic modules used to encrypt and decrypt data.
HOST INTRUSION DETECTION SYSTEM (HIDS)	A detection system that monitors and analyzes internal computing systems for evidence of attack activity.
INCIDENT CONTAINMENT	Removing infected systems from the network as quickly as possible to stop an attacker's movement through a network and prevent further damage.
INCIDENT RESPONSE PLAN	Procedures for reacting to a cyberattack (referred to as an incident) in ways that minimize the damage and enable the election department to recover as quickly as possible.
INFRASTRUCTURE	All components that enable and secure the network including devices, firewalls, and Internet connectivity.

MALWARE	Software that contains a virus to infect systems allowing attackers to steal or destroy data.
MULTIFACTOR AUTHENTICATION (MFA)	A security control that requires more than one way to verify a user’s identity before allowing login.
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)	A recognized authority on security that establishes standards widely followed in the cybersecurity industry.
NETWORK	The group of devices such as computer systems, printers, tablets, and servers linked together wirelessly and/or with cables.
NETWORK PORT	A number that identifies a connection point in the network.
NETWORK SEGMENTATION	Dividing the network into portions separated from the rest of the network to limit access if an attacker gets into the network and manage traffic flow.
NETWORK SWITCH	Hardware device that directs incoming data from multiple input ports to its intended destination.
NEXT-GENERATION FIREWALL (NGFW)	A system that blocks unauthorized network traffic and offers additional functionality such as inspecting applications and preventing intrusions.
PATCH MANAGEMENT	Adhering to a schedule of checking for software and system updates and installing them to ensure the most current cyberattack protections are in place.
PLAN	A detailed step-by-step process defining how election departments will handle specific situations to achieve objectives.
POLICY	Established protocols related to an objective that define how staff should perform activities and manage resources.
PORT SCAN BLOCKING	Preventing attackers from scanning the network to find open ports they can use to get inside the network.
PRINCIPLE OF LEAST PRIVILEGE	A system, application and data access control practice that limits each user’s access to only the needed levels.
RANSOMWARE	A form of malware in which the attacker demands payment to restore the system and data.
REMEDIATION	Fixing security gaps and improving defenses.
REMOVABLE MEDIA	Storage devices that can be removed from a computer while the system is running such as USB keys or drives, CDs, and DVDs.
SECURE SOCKET LAYER (SSL)	A technology that establishes an encrypted link between a website and a browser.
SECURITY INCIDENT AND EVENT MANAGEMENT (SIEM)	Software that collects data generated by systems, security devices and applications that could indicate attack attempts. Security Analysts review the data to determine if a threat is present.
SERVICE SET IDENTIFIER (SSID)	A sequence of characters that uniquely names a wireless local area network (WLAN.)
SOCIAL ENGINEERING	An attack in which a cybercriminal gains access to systems or the network by pretending to be a legitimate voter or citizen to trick an employee into providing usernames and passwords or other access information.
SOFT TOKENS	A software-based multifactor authentication method compared to hard token key FOB or smart card.

STATEFUL DEEP PACKET INSPECTION	A firewall technology that monitors active connections to determine what should be allowed past the firewall.
SYSTEM OR APPLICATION ADMINISTRATOR ACCESS	An account for an application, email or website domain, or system that provides the user with full functionality enabling them to manage other user accounts, enable or block access and make configuration changes.
UTILITIES	Software programs that add functionality to computers or systems.
VENDOR RISK MANAGEMENT POLICY	Protocols that ensure third-party vendors are not introducing security gaps that bad actors can exploit to stage an attack.
VIRTUAL PRIVATE NETWORK (VPN)	An encrypted connection over the Internet that provides secure access for remote computers or devices.
VULNERABILITY SCANNING	An inspection of computers and networks to identify security holes that an attacker could exploit.
WEB APPLICATION FIREWALL (WAF)	Software, a device or service that filters, monitors and blocks malicious traffic from entering a website as well as preventing unauthorized data from leaving a website.
WEB SERVER	A computer system that runs websites. It includes a program that distributes web pages as website visitors click on page web addresses.
WI-FI PROTECTED ACCESS 2 (WPA2)	Security protocol that secures wireless computer networks by using Advanced Encryption Standard (AES), a stronger encryption technology than previous versions.
WRITTEN INFORMATION SECURITY POLICY (WISP)	A set of policies and plans that define how to protect elections from cyberattack and how to respond if an incident occurs. It authorizes employees to quickly perform the described actions without waiting for approval during an attack.