EXHIBIT
tabbies
3

HOPKINS COUNTY
ELECTION INFORMATION
SECURITY POLICY

DOCUMENT MANAGEMENT

The Election Information Security Policy must be reviewed at least once per year or more frequently if state or federal legislation mandates new election security requirements or new cyber threats require policy changes between yearly reviews.

Maintain a record of all policy reviews in the Policy Review Log to validate that the Election Information Security Policy is updated once per year and to track significant revisions. Record all review dates. If major revisions are made during the review, please describe the changes. If changes are not made during a review, note that no changes were made.

POLICY REVIEW LOG

POLICY ADOPTED DATE 7/24/2023				
Drafted By	Tracy Smith, Hopkins County Clerk	Signature	Tracy Smith	7/24/2023
Approved By	Robert Newsom, Hopkins County Judge	Signature	Robert Newsom	7/24/2023
REVIEW AND REVISION LOG				
REVIEW SCHEDULE	• General Election Years: December after elections		• Legislative Session Years:July after SoS Law Conf	

Review Date	If Revised, Revision Date	Revision Description (Or Specify "No Revisions" If None Made)	Drafted By: Name, Title	Signature, Date	Approved By: Name, Title	Signature, Date

Contents

CONFIDENTIAL INFORMATION WARNING

This document contains information about the security of *Hopkins County* that is classified as 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 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.

The following types of confidential information may be contained in this Policy:

System names and purposes

Security device configuration information

Procedural information that could be used to compromise agency systems

NON-DISCLOSURE STATEMENT

The information in this document is Confidential, and cannot be reproduced, redistributed in any way, shape or form without prior written consent from *Hopkins County.*

INTRODUCTION

The *Hopkins County* Election Information Security Policy defines the security policies required to protect technology, data and operations from the cyberattacks threatening elections. The Policy incorporates the Security Best Practices developed by the Texas Secretary of State (SOS) in compliance with HB1421 (2019) legislation adopted to protect elections from cyber threats. It is also aligned to the five core objectives outlined in the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF):

- IDENTIFY (ID)
- PROTECT (PR)
- DETECT (DE)
- RESPOND (RS)
- RECOVER (RC)

This Policy is a living document that is regularly updated as *Hopkins County* builds stronger defenses, addresses new cyber threats, and adapts to changing technology.

POLICY SCOPE

- The Policy applies to any individual and entity participating in any capacity in the management, operation and support of *Hopkins County* elections, election systems and technology.
- The Policy applies to technology, data management, election processes and staff behaviors.
- The Policy encompasses all systems, devices and computers that transmit, receive, and store information used by and for *Hopkins County.*
- The Policy meets applicable federal, state and local laws in addition to *Hopkins County* policies, regulations and contractual obligations.

SECTION 1: IDENTIFY

POLICY 1: GOVERNANCE

Hopkins County follows the guidelines and practices defined in our Election Written Information Security Program (WISP), of which this policy document is a part.

POLICY STANDARDS

- Maintain an updated and authorized Election Written Information Security Program (WISP) which is a set of documents comprised of these five documents:
    1. Election Information Security Policy
    2. Cybersecurity Incident Response Plan
    3. Continuity of Operations Plan
    4. Election System Security Plan
    5. Vendor Risk Management Policy
- Current and future versions of Election WISP policies and plans are approved by Commissioner's Court to ensure that staff has the pre-authorization needed to prevent a cyberattack or take immediate action during an incident. Election WISP policies and plans can be approved as a set of all five documents or they can be approved individually, especially if major revisions are made to only one document.
- The digital version of the Election WISP is stored in CC Office Share and access is limited to election staff only.
- An up-to-date printed copy of the Election WISP is stored in a binder located in Clerk's Office Safe. If the digital version is inaccessible during a cyberattack, the printed version should be retrieved by election staff only.
- All policies and plans in the Election WISP are reviewed and updated according to the following schedule:
    - During general election years, in December after an election to incorporate lessons learned or changes to the election process
    - During legislative session years, in July after the Secretary of State Election Law Conference to incorporate any new laws
- The Policies in the Election WISP apply to any individual and entity participating in any capacity in the management, operation and support of elections, election systems and technology.
- Security responsibilities by employee role are assigned and approved by the Election Administrator. They are documented and tracked using the Security Roles and Responsibilities Chart.

POLICY 2: BUSINESS ENVIRONMENT

Hopkins County clearly states our elections mission and identifies the operations critical to accomplishing it. Security decisions are focused on protecting the operations that support the mission.

To provide our community with safe, secure and accurate elections with the highest level of integrity and transparency.

Voter Registration

Providing Voter and Candidate Information to the Community

Ballot Creation and Loading Ballots to Voting Machines

Ballot by Mail Operations

Poll Worker Coordination and Communication

Transportation of Voting Machines and Ballots to and from Polling Locations

Voter Check-In and Verifying Identity and Eligibility

Secure Transmission of Voter Data to Polling Locations and from Central Servers in Real Time

Unofficial Results Tabulation

Deliver Results to the Public

Canvass of Official Results

Secure Storage of Voting Devices, Election Records, and Electronic Media During the Preservation Period

POLICY STANDARDS

- Our mission statement and the operations critical to accomplishing our mission are clearly defined in written form. NOTE: This mission statement is not a security statement; it is a statement that defines our overall purpose so that we can make security decisions that best protect our ability to fulfill this mission.
- The mission statement and critical operations list must be reviewed as part of the annual Election WISP review required in Policy 1 to make sure they are current and accurately reflect the operations with the most potential to disrupt elections if they are compromised by a cyberattack.

- When writing or updating plans such as the Continuity of Operations Plan, the Incident Response Plan and the Election System Security Plan, the mission statement and critical operations list must be referenced to make sure the plans address the protection and recovery of operations that support our mission.
- The mission statement and critical operations list are included in the Information Security Awareness Training required in Policy 10.

POLICY 3: SECURITY RISK ASSESSMENT AND MANAGEMENT STRATEGY

The election team stays informed of cybercrime targeting elections and takes steps to manage those risks.

POLICY STANDARDS

- A subscription to the Department of Homeland Security Multi-State Information Sharing and Analysis Center (MS-ISAC) and the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) information sharing services must be continuously maintained.
- The processes outlined in our Threat and Risk Monitoring Log worksheet (sample in the Appendix B) must be followed to stay informed of, record and act on MS-ISAC, EI-ISAC and media reports of cyber threats that specifically pose a potential threat to the organization.
- The risk of significant threats to the critical operations that support the mission statement and the overall election process must be assessed as soon as we receive reports of new threats.

POLICY 4: SUPPLY CHAIN RISK MANAGEMENT

Third-party vendors must comply with the Vendor Risk Management Policy included in the Election WISP.

POLICY STANDARDS

- The Vendor Risk Management Policy must be reviewed updated if needed at least yearly as part of the Policy 1 Election WISP annual review requirement.
- Vendor risk should be evaluated annually by checking with vendors to see if any significant changes to their networks, technologies or business processes have recently occurred and by staying informed of cyber threat risks that could affect our vendors via the ISAC information sharing subscription.
- All contracts, supply agreements and service level agreements will specify that the vendor agrees to comply with the Vendor Risk Management Policy.
- A staff escort is required for third-party vendors visiting our facilities, and vendors who regularly work in our facilities are required to have identification badges without unlocking or door access capabilities.
- Vendor risk will be evaluated annually as part of the Election WISP review described in Policy 1.

POLICY 5: ASSET MANAGEMENT

An inventory of devices, systems, equipment, software and data ranked by criticality is created and maintained by the Elections Department and/or IT.

POLICY STANDARDS

- An accurate inventory of election systems must be created and updated annually following the Inventory
- Create and annually update an inventory of all general technology assets including:
  - Election Authority-issued Employee Devices (laptops, desktops, tablets)
  - Servers and Storage Devices
  - Software Including Cloud Software
  - Network Equipment (firewalls, routers, switches, monitoring systems)
- The IT team's inventory must uniquely identify each technology asset by including:
  - Model
  - Serial Number
  - Location
- The inventory ranks the criticality of each asset using the Technology Asset Criticality Classification System in Table 1 that reflects the importance of each technology asset to mission-critical operations.
- The inventory includes chain of custody information for critical assets such as:
  - Person who issued the item
  - Person using the item
  - Person receiving the item when it's returned
- The inventory must include a change management log documenting significant updates, patches and changes made to critical assets.
- Each asset is managed according to security guidelines defined in the Technology Asset Criticality Classification System in Table 2 below.
- Removable media devices should be included in the inventory, and their use and management must comply with the Removable Media Policy. An example of a Removable Policy is in the Appendix D.
- A diagram depicting the network design and data flow of critical operations must be created and stored with the asset inventory.

TABLE 1: TECHNOLOGY ASSET CRITICALITY CLASSIFICATION SYSTEM

CRITICALITY LEVEL	ASSETS INCLUDED, BUT NOT LIMITED TO	SECURITY GUIDELINES
1	Servers storing voter and candidate information Election systems ePollbooks Website Server and/or Hosting Account Voter Registration System Account Encrypted Backup Hard Drive	• Physical Assets ○ Assets must be stored in a locked location ○ A two-person verification record in an access log is required for entry to area ○ Access is limited to authorized personnel only ○ Written approval must be obtained before access to the area is granted ○ Physical assets in offsite locations such as IT vendor facilities must be stored in a locked area with restricted and controlled access • Software Assets ○ Access is limited to authorized personnel only with strict limitations on who receives administrator privileges ○ Written approval is required before access credentials or administrator privileges will be granted ○ Unique usernames must be used ○ Credential sharing is strictly prohibited ○ Strong passwords are required ○ Multifactor authentication is required where possible ○ On premise assets must be contained within the election network firewall

		○ Remote and Internet access is restricted ○ Continuous monitoring for suspicious activity is required ○ Data must be backed up using encryption ○ Chain of custody record is required
2	Employee desktops and laptops Mobile devices Productivity Software Social media accounts	• Physical Assets ○ Protect physical access to hardware assets by keeping them in a locked area when not in use ○ Assignment log is required ○ Limit area access to personnel or escorted visitors only • Software Assets ○ Approval process not required, but access credentials should be assigned to personnel only ○ Assign unique usernames and prohibit credential sharing ○ Require strong passwords ○ Require multifactor authentication where possible ○ Keep the asset located behind election-specific firewall in the network ○ Remote access via a Virtual Private Network permissible ○ Monitor for suspicious activity ○ Backup data using encryption
3	Printers Copy Machines Fax machines	• Locked area not required, but advised • Require strong passwords if needed • Multifactor authentication not required

		- Monitor for suspicious activity

SECTION 2: PROTECT

POLICY 6: DATA SECURITY AND INFORMATION PROTECTION

The Election Data Classification System must accurately include all election data types and correctly categorize the data according to how stringently it should be protected. Election-related data must be inventoried, labeled and secured consistent with the Election Data Classification System (Table 2).

POLICY STANDARDS

- An accurate inventory of all major data sets that are managed, stored and used to support elections must be created and annually updated using the Technology Asset Inventory, Classification, Chain of Custody and Change Management Log in the Appendix C.
- The data inventory must include classification levels of election data according to the Election Data Classification System in Table 2 below.
- Data will be consistently backed up to a system that is_not connected to the Internet or the election network and that is stored offsite
- Encryption must be used to protect Confidential, Sensitive and Internal Use election data as it is sent between systems and offices and while it is stored.
- Confidential, Sensitive and Internal Use data must be permanently deleted from decommissioned computers, devices, servers, hard drives and removable media before they are disposed or reused.
- Removable media devices such as USB keys temporarily used to transfer data classified as Confidential or Sensitive between devices should be erased as soon as possible after use.
- Servers, storage devices and computers storing Confidential or Sensitive information must be erased before releasing them to external third-party vendors for maintenance.
- IT equipment, systems and devices must be stored and used in temperature-controlled facilities with access to the area protected by locks and visitor management processes such as badges and/or staff escort.
- The data security processes will be reviewed annually as part of the Election WISP review prescribed in Policy 1.
- Data security processes must comply with all current or future information security federal and state regulations and laws, including the Texas Public Information Act, and the Records Management Retention and Disposition Schedules issued by the Texas State Library Archives Commission (TSLAC).

TABLE 2: ELECTION DATA CLASSIFICATION SYSTEM

DATA CLASSIFICATION LEVEL	DATA TYPE
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 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.

	○ Voter Registration Data Disclosing Criminal History or Voter Activity/Inactivity ○ 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 job duties. Data in this category may become available to the public, if a public information request or inquiry is received and approved.	• 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 ○ 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	• Election News and Announcements • Job Announcements • Election System and Voting Equipment Types • Voting System Type • Poll Locations

declared public knowledge by someone with the proper authorization and should not be used or disclosed without approval.	• Election Schedules • Ballot Information • Tabulation Results • Official Domain URLs

POLICY 7: IDENTITY MANAGEMENT, AUTHENTICATION AND ACCESS CONTROL

Access to data, assets and facilities is limited to authorized users and follows the election data and asset classification systems if applicable.

POLICY STANDARDS

- Access to systems, computers and devices will be granted according to two classifications:
  - User - Granted to authorized personnel only.
  - Administrator – Administrator access must be approved by the (Specify the approval authority, such as Election Administrator.)
- Access to data and software must be assigned to users based on their roles to ensure each user only has access to the information required to perform job duties (See Appendix H).
- Shared user accounts are not permitted. A unique username is required for each user's access to systems, computers and devices as well as data and software functionality.
- All remote access sessions must use encryption and multifactor authentication when possible.
- Inactive user and administrator accounts will be disabled unless an exception is approved by the Election Administrator.

POLICY 8: ELECTION INFORMATION SYSTEM MAINTENANCE

Maintenance and repairs of information system components should be performed regularly and logged. These systems include all voting technologies, ePollbooks, computers, and servers used to support elections.

POLICY STANDARDS

- Changes to election information systems and network architecture as well as chain of custody information must be tracked in the Technology Asset Inventory, Classification, Chain of Custody and Change Management Log. An example is in the Appendix C.
- Preventative maintenance will be performed at a frequency that is equal to or greater than that suggested by the manufacturer and maintenance procedures will be documented in the Technology Asset Inventory, Classification, Chain of Custody and Change Management Log. An example is in the Appendix C.
- Systems removed from the network for maintenance and repair, either onsite or at an offsite facility, must be tested after the services are completed by running an anti-virus scan before they can be reconnected to the network.
- Maintenance agreements through third-party contracts must follow the Vendor Risk Management Policy.
- Maintenance performed by third parties on information systems via remote access tools must be monitored via screen sharing for the duration of the remote session.
- Annual network penetration testing is required. During years in which an Election Security Assessment is conducted, the penetration test performed as part of the assessment satisfies this requirement.
- Annual vulnerability scanning is required for all assets connected to the network. The vulnerability scan performed as part of an Election Security Assessment satisfies this requirement.

POLICY 9: USE OF PROTECTIVE TECHNOLOGY

Technology is used to prevent unauthorized access to data or technology, malware and ransomware infection and to secure information systems against disruptions, cyberattacks and equipment failure.

POLICY STANDARDS

- Email is protected by SPAM and malware filters.
- Internet content filtering should be used to block access to sites with potential viruses.
- An Endpoint Protection Solution should be used to protect computers, devices and systems from malware, ransomware and unauthorized access.
- Next-generation firewalls with encryption capabilities should be used to protect the network.
- Network segmentation must be implemented to separate critical election data sets and functionality from non-elections segments of the network and other department networks.
- Systems and devices must be configured with the least amount of functionality needed to perform assigned tasks to ensure that each user does not have more capability or than needed.
- All personal devices including USB drives, smartphones, cameras and music players must never be connected to the network unless approved by the <u>Election Administrator</u> and devices must be managed in compliance with the Removable Media Policy.

POLICY 10: INFORMATION SECURITY AWARENESS TRAINING

Personnel and partners participate in cybersecurity awareness training to ensure everyone understands their information security-related responsibilities and how to protect election data and technology.

POLICY STANDARDS

- Each member of the election staff is required to participate in the training offered by the Texas Secretary of State.
- Training for new users will take place no less than 30 days from their hire date and repeated annually thereafter.
- In addition to the general security content, training will include the Election WISP, including the Election Security Incident Response Plan, Continuity of Operations Plan, Data and Asset Classification Systems, Removable Media Policy and Security Roles and Responsibilities as well as any information relevant to specific roles.
- The team should have frequent discussions about security practices to build a culture of physical and cybersecurity.
- Training records must be retained with human resources files for the amount of time allotted in the record retention requirements.

SECTION 3: DETECT

POLICY 11: CONTINUOUS SECURITY MONITORING

Network traffic, assets and physical access are monitored to identify cyberattack activities and verify the effectiveness of protective measures.

POLICY STANDARDS

- Monitoring must be conducted either internally or by contracting with a service to monitor and detect possible cyberattack activities across potential attack points including:
  - Network
  - Mobile access to the network
  - Third-party vendor interactions with the network and connected systems
- Monitoring activity must be conducted to detect unauthorized:
  - Connections
  - Devices
  - Software
  - Personnel
  - Code
  - Mobile access

POLICY 12: DETECTING ANOMALIES AND EVENTS

User behaviors and network traffic patterns that fall outside the normal pattern of activity must be identified quickly and analyzed to determine if these anomalies indicate a cyberattack.

POLICY STANDARDS

- As part of the monitoring process, normal network activity should be documented and used as a comparison point to detect anomalous activity that could indicate a security incident.
- The Election Security Incident Response Plan should document the activity that indicates an active attack and triggers activation of the Election Security Incident Response Plan.
- The impact potential of cyberattacks is determined and included in the Election Security Incident Response Plan to ensure that it is understood by personnel.

POLICY 13: DETECTION PROCESSES

Election and IT staff members are required to be vigilant in recognizing unusual activity that could be an indicator of a cyberattack, and suspicious activity must be immediately reported.

POLICY STANDARDS

- Election staff threat detection responsibilities are clearly defined to ensure staff know what they are expected to do to identify, report, and assist in the response to potential cyber threat activity. See the Election Security Roles and Responsibilities worksheet in Appendix B.
- Potential incidents must be reported immediately to either Kaybro IT or the Elections Administrator
- The effectiveness of staff detection processes and Security Roles and Responsibilities must be reviewed annually as part of the Election WISP review prescribed in Policy 1. An example of the Security Roles and Responsibilities is in the Appendix A.
- Training staff on detection responsibilities and processes must be included in the Security Awareness Training required in Policy 10.
- Anti-virus software must be installed on laptops and devices that are in operation at all times.

SECTION 4 OBJECTIVE: RESPOND

POLICY 14: RESPONSE PLANNING

An up-to-date and authorized Incident Response Plan is maintained, made available to staff and followed in the case of a security incident.

POLICY STANDARDS

- An Election Security Incident Response Plan should be annually updated and maintained as part of the approved Election Written Information Security Program as defined in Policy 1.
- The Election Security Incident Response Plan includes processes to identify, contain, and eradicate active incidents as well as recover and implement improvements after the incident.
- The Election Security Incident Response Plan should be stored in digital and printed format with the other Election WISP documents as descripted in Policy 1.
- Information Security Awareness Training as defined in Policy 10 must include the Election Security Incident Response Plan.
- The Election Security Incident Response Plan should be added to the local government Emergency Response Plan.
- An Incident Response Team must be formally created with clearly described roles and responsibilities in the Election Security Incident Response Plan. The team should include *Election Administrator, IT Vendor, Emergency Management Coordinator, County Judge* and members of the team should always be familiar with the plan and ready to respond to an incident.
- The Election Security Incident Response Plan must define incident preparation and all preparedness activities must be completed including gathering needed information in a single location and assembling equipment and resources that will be needed to respond to an incident.
- Every two years, Table-Top Exercises should be conducted that simulate an active incident so as to provide election staff with practice in executing the Election Security Incident Response Plan.

POLICY 15: ANALYSIS

Each security incident is analyzed to determine severity and scope and to ensure the right resources and stakeholders are assembled to address the full impact of the incident.

POLICY STANDARDS

- The Election Security Incident Response Plan must include a process for analyzing the cause and impact of an incident in consideration of the fact that some cyberattacks will be further reaching and more severe than others.
- Incidents should be categorized based on the severity of their impact on operations to guide the scope of response efforts.
- The analysis must include a review of potential third-party involvement to determine if response activities should incorporate third-party incident response policies and stakeholders.
- Evidence must be preserved to provide a court of law or cybersecurity insurance providers with needed information for prosecution and handling insurance claims. Evidence should be retained according to the duration specified for records retention in the election code.
- Using the information collected in the Incident Handler's Log included in the Election Security Incident Response Plan, an incident report must be completed for each incident that falls into the severity categories of Critical and High and submitted to the Texas Secretary of State Office.

POLICY 16: MITIGATION OF CYBERATTACKS

Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.

POLICY STANDARDS

- Incidents must be immediately blocked and contained according to the processes outlined in the Election Security Incident Response Plan.
- As soon as an active incident is confirmed, the Election Administrator must notify all election staff members and assemble the Incident Response Team according to the notification process defined in the Election Security Incident Response Plan.
- The Incident Response Team must immediately follow the mitigation steps outlined in the Election Security Incident Response Plan.
- The damage caused by an incident must be repaired as soon as possible, with priority recovery given to the mission statement and critical operations list defined in Policy 2.
- Backup data should be available and used to restore functionality and operations as described in the Election Security Incident Response Plan.

POLICY 17: RESPONSE COMMUNICATIONS

Response activities are coordinated with internal and external stakeholders including law enforcement agencies, insurance providers, IT service providers and public relations resources as defined in the Election Security Incident Response Plan.

POLICY STANDARDS

- A communication plan is included in the Election Security Incident Response Plan and Continuity of Operations Plan that encompasses both internal and external communications during a cyberattack incident.
- Each stakeholder must receive only the information they are authorized to receive according to Election Data Classification System defined in Policy 6.
- The communication plan should be aligned with information-sharing guidance from the public affairs office, legal department and leadership officials. As these entities make changes to their information-sharing guidelines, the Election Security Incident Response Plan must be updated to incorporate the new information.
- Public-facing communication about the incident should be distributed only through official election sources, such as the Election Authority's website. Press should be advised to only report ~~only~~ information that can be confirmed with the official Election Authority website.
- Social media should not report detailed information to avoid followers changing information as they share it. Social media should only direct followers to the Election Authority's website for all information.
- Clearly defined communication roles and responsibilities must be included in the Election Security Roles and Responsibilities list. An example is in the Appendix A.
- Incidents must be reported as required by laws and regulations which are defined in the Election Security Incident Response Plan.

POLICY 18: RESPONSE IMPROVEMENTS

Response procedures in the Election Security Incident Response Plan must be continuously improved by incorporating lessons learned from real and practice incident detection and response activities.

POLICY STANDARDS

- The Incident Response Team should meet one month or less after a security incident occurs or Table-Top Exercises have been completed to provide input and feedback on lessons learned.
- New practices or cyberattack defenses that emerge from the lessons learned must be added to the Election Security Incident Response Plan, the Continuity of Operations Plan and any other plans or policies in the Election WISP, as needed.
- If significant changes to any of the documents in the Election WISP are required to address response lessons learned, particularly changes that require additional resources and funding, the updated plan or policy should be approved and authorized by Commissioner's Court.

SECTION 5 OBJECTIVE: RECOVER

POLICY 19: RECOVERY PLANNING

Recovery processes and procedures should be executed and maintained to ensure timely restoration of systems or assets affected by cyberattacks.

POLICY STANDARDS

- The Continuity of Operations Plan (COOP) must be followed immediately during a cyberattack to minimize disruption and continue to serve our mission.
- The recovery activities in the Election Security Incident Response Plan must be followed to enable a return to normal operations as quickly as possible.
- Recovery activities in all plans and policies should be reviewed at a minimum annually as part of the Election WISP review prescribed in Policy 1, and more frequently if needed after a Table-Top Exercise and after a cyberattack.
- Following significant changes made to organizational structure, election processes and technology infrastructure, the Election WISP should be updated with recovery activities aligned to the new information. Significant changes are those that add or remove resources and assets that must be protected from cyberattack and restored if they are disrupted by an attack.
- If significant changes to any of the documents in the Election WISP are required to address new or different recovery activities, particularly changes that require additional resources and funding, the updated plan or policy should be approved and authorized by Commissioner's Court.

POLICY 20: RECOVERY IMPROVEMENTS

The recovery procedures in the Election Security Incident Response Plan and the Continuity of Operations Plan must be continuously improved by incorporating lessons learned from incident recovery activities.

POLICY STANDARDS

- The Incident Response Team should meet one month or less after a security incident occurs or Table-Top Exercises have been completed, to provide input and feedback on lessons learned in executing recovery activities.
- New or obsolete recovery practices that emerge from the lessons learned must be added to the Election Security Incident Response Plan, the Continuity of Operations Plan and any other plans or policies in the Election WISP as needed.
- If significant changes to any of the documents in the Election WISP are required to address recovery lessons learned, particularly changes that require additional resources and funding, the updated plan or policy should be approved and authorized by Commissioner's Court.

POLICY 21: RECOVERY COMMUNICATIONS

Restoration activities should be coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of affected systems, particularly systems spreading malware or other attack damage, additional victims and vendors.

POLICY STANDARDS

- A recovery communications plan must be a component of the Election Security Incident Response Plan to facilitate both internal and external communications during and after a cyberattack. The communications plan should ensure that each group of internal and external stakeholders only receives the information they are authorized to receive as defined in the Data Classification System in Policy 6.
- Public-facing communication about the recovery should be distributed only through official election sources, such as the website. Press should be advised to report only information that can be confirmed with the official Election Authority's website.
- Social media should not report detailed information to avoid followers changing information as they share it. Social media should only direct followers to the Election Authority's website for information.
- The communications plan should include public relations management after the cyberattack itself and then again after recovery. These two intervals of communication allow your entity to correct misinformation and to repair trust that may have been damaged during the incident.

APPENDIX A: ROLES AND SECURITY RESPONSIBILITIES

Role	Security Responsibility
Election Administrator	• Ensure the Election WISP is accessible only to election staff and all employees know where to find it and how to access it. • Ensure the Election WISP is approved and authorized by leadership. • Coordinate Election WISP reviews and updates in December after an election and in June after a legislative session. • If new cyber threats are identified, ensure that Election WISP policies and plans are updated with practices that protect against them. • Notify IT or cybersecurity resources of any reports from staff of suspicious activity or events that could indicate an active attack incident. • Notify the Texas Secretary of State Election Team if the activity is determined to be a true threat that requires activation of the Election Security Incident Response Plan. • Notify the Texas Department of Information Resources if the activity is determined to be a true threat. • Conduct an annual review of changes to operations and if the changes introduce new opportunities for cyberattacks. • Ensure that the most current version of the Election WISP is covered in the mandatory annual employee security awareness training curriculum.
All Election Staff	• Remain vigilant for indicators of a cyberattack. • Report suspicious activity to the Election Administrator who will immediately notify IT and/or security resources to determine if the activity indicates an active cyber threat. • Annually participate in security awareness training and Table-Top Exercises. • Know where to find the Election WISP. • Be familiar with the Election WISP and understand what to do to help protect operations, data and systems and how to respond to an incident. • Follow news about security threats and cybercrime trends and understand their potential impact to your elections.

Supply Manager	• Ensure that vendor contracts include the requirement to follow the Election Information Security Policy and the Vendor Risk Management Policy. • Ask vendors to provide security assessment results that include their security policies, plans and practices and store them with the vendor contract. • If a vendor is not following the Vendor Risk Management Policy, provide a reasonable timeframe to establish compliance. If the policy is still not being followed after the time period ends, consider changing vendors to engage with a vendor with the needed security practices.
Office Manager	• Maintain an up-to-date inventory of assets. • Require that visitors to the facility sign into a visitor log book, have name tags, and are escorted by staff. • Ensure that facilities are locked, and surveillance camera video is properly recorded and stored according to retention policies.
IT Manager	• Implement the data security requirements in the Security Best Practice Guidelines, Election Information Security Policy and the Election Systems Security Policy. • Monitor cyber intelligence feeds from MS-ISAC/EI-ISAC and the media for cyber threat trends that could impact elections and require defense adjustments.
Voter Registrar	• Adhere to the Election Information Security Policy and the Elections Systems Security Policy. • Report suspicious activity to the Election Administrator who will immediately notify the appropriate entities to determine if the activity indicates an incident. • Annually review changes to the voter registration process and determine if the changes introduce new opportunities for cyberattacks that require additional or new security practices or render some existing practices obsolete. • Communicate voter registration process changes to the Election Administrator and request that the changes be incorporated into Election WISP if needed.
Tax Collector	• Adhere to the Election Information Security Policy and the Elections Systems Security Policy. • Report suspicious activity to the Election Administrator who will immediately notify the appropriate entities to determine if the activity indicates an incident. • Annually review changes to the tax collection process and determine if the changes introduce new opportunities for cyberattacks that require additional or new security practices or render some existing practices obsolete.

	- Communicate tax collection process changes to the Election Administrator and request that the changes be incorporated into the Election WISP if needed.