

# PANOLA COUNTY SHERIFF'S OFFICE

Office: 903-693-0333  
Fax: 903-693-9366



314 W. Wellington  
Carthage, Texas 75633

November 27, 2023

**Sheriff Cutter Clinton**

The Honorable Rodger McLane  
Panola County Judge  
110 S. Sycamore  
Carthage, Texas 75633

Dear Judge McLane,

Please add the following item(s) to the next scheduled meeting of the Panola County Commissioner's Court:

Please record the increase in rate of pay for Sean Howard, a Detention Officer for the Panola County Sheriff's Office from \$16.81 per hour to \$18.11 per hour effective December 2, 2023.

Sincerely,

A handwritten signature in black ink that reads "Cutter Clinton". The signature is stylized with a large, sweeping initial "C".

Cutter Clinton  
Sheriff

CC/lw  
CC: Jennifer Stacy  
Joni Reed


**Honesty, Integrity, Service**

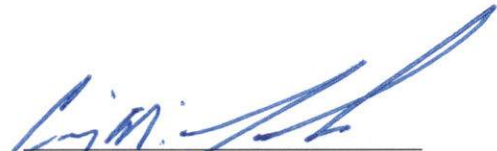
**PANOLA COUNTY  
2023  
BUDGET AMENDMENT #15**

We hereby amend the Panola County Budget for the Fiscal Year 2023 as set forth above according to the procedures outlined under Local Government Code, Chapter 111, Subchapter A Sections 111.010 (c), (d). A copy of this Order is to be filed with the County Clerk and Attached to the Budget originally adopted for 2023.

Signed on this 5th day of December, 2023.

  
\_\_\_\_\_  
County Judge

  
\_\_\_\_\_  
Commissioner Precinct # 1

  
\_\_\_\_\_  
Commissioner Precinct # 3

  
\_\_\_\_\_  
Commissioner Precinct # 2

  
\_\_\_\_\_  
Commissioner Precinct # 4

Passed and approved by the Commissioners Court of Panola County on the 5th day of December, 2023 as the same appears on file in the office of the County Clerk of Panola County.

  
\_\_\_\_\_  
County Clerk





Panola County, Texas

# Budget Adjustment Register

## Adjustment Detail

Packet: GLPKT19854 - #14 12-5-2023

Adjustment Number	Budget Code	Description	Adjustment Date
BA0001996	2023 PANOLA COUNTY BU...	646-AUTOPSIES & INQUEST	11/28/2023

**Summary Description:**

Account Number	Account Name	Adjustment Description	Before	Adjustment	After
<a href="#">100-409-54120</a>	INSURANCE/ LIAB. FIRE ETC.	646-AUTOPSIES & INQUEST	400,395.00	-30,000.00	370,395.00
November:					
				-30,000.00	
<a href="#">100-646-54770</a>	AUTOPSIES AND INQUESTS	646-AUTOPSIES & INQUEST	80,000.00	30,000.00	110,000.00
November:					
				30,000.00	



Panola County, Texas

# Budget Adjustment Register

## Adjustment Detail

Packet: GLPKT19857 - #15 OPTIONAL TCDRS CONTRIBUTION

Adjustment Number	Budget Code	Description	Adjustment Date
BA0001997	2023 PANOLA COUNTY BU...	OPTIONAL TCDRS CONTRIBUTION	11/29/2023

**Summary Description:**

Account Number	Account Name	Adjustment Description	Before	Adjustment	After
<a href="#">200-360-41001</a> November: -50,000.00	INTEREST EARNINGS	OPTIONAL TCDRS CONTRIBUTION	-198,273.00	-50,000.00	-248,273.00
<a href="#">200-621-52130</a> November: 12,500.00	OPTIONAL RETIREMENT CONT	OPTIONAL TCDRS CONTRIBUTION	31,305.00	12,500.00	43,805.00
<a href="#">200-622-52130</a> November: 12,500.00	OPTIONAL RETIREMENT CONT	OPTIONAL TCDRS CONTRIBUTION	31,305.00	12,500.00	43,805.00
<a href="#">200-623-52130</a> November: 12,500.00	OPTIONAL RETIREMENT CONT	OPTIONAL TCDRS CONTRIBUTION	31,305.00	12,500.00	43,805.00
<a href="#">200-624-52130</a> November: 12,500.00	OPTIONAL RETIREMENT CONT	OPTIONAL TCDRS CONTRIBUTION	31,305.00	12,500.00	43,805.00





Panola County, Texas

# Budget Adjustment Register

## Adjustment Detail

Packet: GLPKT19859 - #15 AIRPORT UTILITIES

Adjustment Number	Budget Code	Description	Adjustment Date
BA0001998	2023 PANOLA COUNTY BU...	407-AIRPORT UTILITIES	11/29/2023

**Summary Description:**

Account Number	Account Name	Adjustment Description	Before	Adjustment	After
<a href="#">100-360-41001</a>	INTEREST EARNINGS	405-AIRPORT UTILITIES	-802,784.00	-1,553.00	-804,337.00
November:	-1,553.00				
<a href="#">100-407-54430</a>	UTILITIES	405-AIRPORT UTILITIES	12,945.00	1,553.00	14,498.00
November:	1,553.00				



Panola County, Texas

# Budget Adjustment Register

## Adjustment Detail

Packet: GLPKT19870 - #15 ELECTIONS PROFESSIONAL SERVICES

Adjustment Number	Budget Code	Description	Adjustment Date
BA0001999	2023 PANOLA COUNTY BU...	ELECTIONS MASS MAIL OUT	12/4/2023

**Summary Description:**

Account Number	Account Name	Adjustment Description	Before	Adjustment	After
<a href="#">100-490-54150</a>	PROFESSIONAL SERVICES	ELECTIONS MASS MAIL OUT	17,925.00	2,000.00	19,925.00
December: 2,000.00					
<a href="#">100-491-53100</a>	OFFICE SUPPLIES & REPAIRS	ELECTIONS MASS MAIL OUT	2,500.00	-340.00	2,160.00
December: -340.00					
<a href="#">100-491-54270</a>	CONFERENCES AND DUES	ELECTIONS MASS MAIL OUT	7,009.00	-1,660.00	5,349.00
December: -1,660.00					



Panola County, Texas

# Budget Adjustment Register

## Adjustment Detail

Packet: GLPKT19871 - #15 CONST. 1 & 4 COMMUNICATIONS

Adjustment Number	Budget Code	Description	Adjustment Date
BA0002000	2023 PANOLA COUNTY BU...	COMMUNICATION TELEPHONE	12/4/2023

**Summary Description:**

Account Number	Account Name	Adjustment Description	Before	Adjustment	After
<a href="#">100-585-54200</a>	COMMUNICATION TELEPHONE	COMMUNICATION TELEPHONE	1,000.00	50.00	1,050.00
December: 50.00					
<a href="#">100-585-54990</a>	MISCELLANEOUS	COMMUNICATION TELEPHONE	500.00	-50.00	450.00
December: -50.00					

Form #2201 Rev. 05/2020

Submit to:

SECRETARY OF STATE

Government Filings

Section P O Box 12887

Austin, TX 78711-2887

512-463-6334

512-463-5569 - Fax

Filing Fee: None



STATEMENT OF OFFICER

FILED FOR RECORD  
IN MY OFFICE

AT 2:40 O'CLOCK P M

DEC 07 2023

BOBBIE DAVIS  
COUNTY CLERK, PANOLA COUNTY, TEXAS

BY B. Davis DEPUTY

Statement

I, Madison Hudnall, do solemnly swear (or affirm) that I have not directly or indirectly paid, offered, promised to pay, contributed, or promised to contribute any money or thing of value, or promised any public office or employment for the giving or withholding of a vote at the election at which I was elected or as a reward to secure my appointment or confirmation, whichever the case may be, so help me God.

Title of Position to Which Elected/Appointed: Deputy Sheriff

Execution

Under penalties of perjury, I declare that I have read the foregoing statement and that the facts stated therein are true.

Date: 11/15/2023

Madison Hudnall  
Signature of Officer

Form #2204 Rev 9/2017

Submit to:  
SECRETARY OF STATE  
Government Filings Section  
P O Box 12887  
Austin, TX 78711-2887  
512-463-6334  
FAX 512-463-5569  
Filing Fee: None



OATH OF OFFICE

This space reserved for office use  
FILED FOR RECORD  
IN MY OFFICE

AT 2:40 O'CLOCK P M

DEC 07 2023

BOBBIE DAVIS  
COUNTY CLERK, PANOLA COUNTY, TEXAS  
BY B. Davis DEPUTY

IN THE NAME AND BY THE AUTHORITY OF THE STATE OF TEXAS,  
I, Madison Hudnall, do solemnly swear (or affirm), that I will faithfully  
execute the duties of the office of Deputy Sheriff of  
the State of Texas, and will to the best of my ability preserve, protect, and defend the Constitution and laws  
of the United States and of this State, so help me God.

Madison Hudnall  
Signature of Officer

Certification of Person Authorized to Administer Oath

State of Texas  
County of Panola

Sworn to and subscribed before me on this 14th day of November, 2023

(Affix Notary Seal,  
only if oath  
administered by a  
notary.)

R. C. Clinton

Signature of Notary Public or  
Signature of Other Person Authorized to Administer An  
Oath

R. C. Clinton  
Printed or Typed Name



National Bond Center  
350 E. 96th Street  
Indianapolis, Indiana 46240  
+1 (888) 8442663 Fax: +1 (866) 5474883

Richard H. Thomas Inc.  
PO Box 430  
Carthage, Texas 75633-0430

Agent Telephone: 903-693-3831  
Bond Number: 999220259  
Cross Reference:

FILED FOR RECORD  
IN MY OFFICE

AT 2:40 O'CLOCK P M

SARAH FIELDS  
206 CR 404  
CARTHAGE, Texas 75633

DEC 07 2023

BOBBIE DAVIS  
COUNTY CLERK, PANOLA COUNTY, TEXAS  
BY B. Davis DEPUTY

We appreciate having you as a Liberty Mutual customer and we would like to thank you for allowing us to serve your bonding needs. This letter is to confirm Liberty Mutual Surety has received payment for your renewing bond.

The effective date of your renewing bond begins 11/23/2023.

Please review the enclosed documents for accuracy. You must remit the original of the New Bond and any supporting documents required to your Obligee.

If you have any questions regarding this bond or would like to discuss your future bond needs, please contact your Liberty Mutual agent.

Again, thank you for entrusting us with your bonding needs.

Sincerely,  
National Bond Center

For additional information regarding Liberty Mutual insurance products, please visit [www.libertymutual.com](http://www.libertymutual.com)





Liberty Mutual Surety
Attention: LMS Claims
P.O. Box 34526
Seattle, WA 98124
Phone: 206-473-6210
Fax: 866-548-6837
Email: HOSCL@libertymutual.com
www.LibertyMutualSuretyClaims.com

PUBLIC OFFICIAL BOND

KNOW ALL MEN BY THESE PRESENTS:

No. 999220259

That we SARAH FIELDS

P.O. Box 127, CARTHAGE, TX 75633

(Insert Full Name [top line] and Address [bottom line] of Principal)

, as Principal and The Ohio Casualty Insurance Company, a corporation organized and existing under the laws of the State of New Hampshire, (hereinafter called the Surety, are held and firmly bound unto Panola County

County Auditors Office Rm 213A, Carthage, TX 75633

(Insert Full Name [top line] and Address [bottom line] of Obligee)

in the aggregate and non-cumulative penal sum of Two Thousand Dollars And Zero Cents

(\$2,000.00)

) DOLLARS, for the payment of which, well and truly

to be made, we bind ourselves, our heirs, executors, administrators, successors and assigns, jointly and severally, firmly by these presents.

WHEREAS, the said Principal has been elected or appointed to (or holds by operation of law) the office of Reserve Deputy

Constable Pct. 1&4

for a term

beginning on November 23, 2023 and ending on November 23, 2024.

Now, therefore, the condition of this Obligation is such that if the said Principal shall well, truly and faithfully perform all official duties required by law of such official during the term aforesaid, then this obligation shall be void; otherwise it shall remain in full force and effect, subject to the following conditions:

First: That the Surety may, if it shall so elect, cancel this bond by giving thirty (30) days notice in writing to Panola County

County Auditors Office Rm 213A, Carthage, TX 75633

and

this bond shall be deemed canceled at the expiration of said thirty (30) days, the Surety remaining liable, however, subject to all the terms, conditions and provisions of this bond, for any act or acts covered by this bond which may have been committed by the Principal up to the date of such cancelation; and the Surety shall, upon surrender of this bond and its release from all liability hereunder, refund the premium paid, less a pro rate part thereof for the time this bond shall have been in force.

Second: That the Surety shall not be liable hereunder for the loss of any public moneys or funds occurring through or resulting from the failure of, or default in payment by, any banks or depositories in which any public moneys or funds have been deposited, or may be deposited, or placed to the credit, or under the control of the Principal, whether or not such banks or depositories were or may be selected or designed by the Principal or by other persons; or by reason of the allowance to, or acceptance by the Principal of any interest on said public moneys or funds, any law, decision, ordinance or statute to the contrary notwithstanding.

Third: That the Surety shall not be liable for any loss or losses, resulting from the failure of the Principal to collect any taxes, licenses, levies, assessments, etc., with the collection of which he may be chargeable by reason of his election or appointment as aforesaid.

SIGNED, SEALED and DATED November 1, 2023.

SARAH FIELDS

Handwritten signature of Sarah Fields

The Ohio Casualty Insurance Company



By: Timothy A. Mikolajewski

Timothy A. Mikolajewski

Attorney-in-Fact

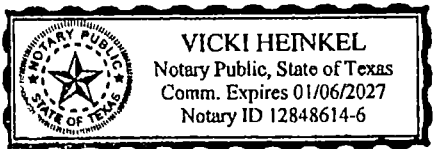
OATH OF OFFICE

STATE OF Texas  
County of Panola } SS

I, Sarah Fields  
do solemnly swear (or affirm) that I will support, protect and defend the Constitution of The United States and the Constitution of the State of Texas and that I will discharge the duties of my office of Reserve Deputy Constable PCT. 144 with fidelity; that I have not paid or contributed, or promised to pay or contribute, either directly or indirectly, any money or other valuable thing to procure my nomination or election (or appointment), except for necessary and proper expenses expressly authorized by law; that I have not knowingly violated any election law of this State, or procured it to be done by others in my behalf; that I will not knowingly receive, directly or indirectly, any money or other valuable thing for the performance or non-performance of any act or duty pertaining to my office than the compensation allowed by law. So help me God.

Sarah Fields

Sworn to and subscribed before me this 17th day of November, 2023



Vicki Heinkel



This Power of Attorney limits the acts of those named herein, and they have no authority to bind the Company except in the manner and to the extent herein stated.

The Ohio Casualty Insurance Company  
**POWER OF ATTORNEY**

Principal: SARAH FIELDS  
Agency Name: Richard H. Thomas Inc. Bond Number: 999220259  
Obligee: Panola County  
Bond Amount: (\$2,000.00 ) Two Thousand Dollars And Zero Cents

KNOW ALL PERSONS BY THESE PRESENTS: that The Ohio Casualty Insurance Company, a corporation duly organized under the laws of the State of New Hampshire (herein collectively called the "Company"), pursuant to and by authority herein set forth, does hereby name, constitute and appoint Timothy A. Mikolajewski in the city and state of Seattle, WA, each individually if there be more than one named, its true and lawful attorney-in-fact to make, execute, seal, acknowledge and deliver, for and on its behalf as surety and as its act and deed, any and all undertakings, bonds, recognizances and other surety obligations, in pursuance of these presents and shall be as binding upon the Companies as if they have been duly signed by the president and attested by the secretary of the Company in their own proper persons.

IN WITNESS WHEREOF, this Power of Attorney has been subscribed by an authorized officer or official of the Company and the corporate seal of the Company has been affixed thereto this 28th day of March, 2021.



The Ohio Casualty Insurance Company

By: *David M. Carey*  
David M. Carey, Assistant Secretary

Not valid for mortgage, note, loan, letter of credit, currency rate, interest rate or residual value guarantees.

For bond and/or Power of Attorney (POA) verification inquiries, please call 610-832-8240 or email HOSUR@libertymutual.com.

STATE OF PENNSYLVANIA ss  
COUNTY OF MONTGOMERY

On this 28th day of March, 2021, before me personally appeared David M. Carey, who acknowledged himself to be the Assistant Secretary of The Ohio Casualty Insurance Company and that he, as such, being authorized so to do, execute the foregoing instrument for the purposes therein contained by signing on behalf of the corporations by himself as duly authorized officer.

IN WITNESS WHEREOF, I have hereunto subscribed my name and affixed my notarial seal at Plymouth Meeting, Pennsylvania, on the day and year first above written.



Commonwealth of Pennsylvania - Notary Seal  
Teresa Pastella, Notary Public  
Montgomery County  
My commission expires March 28, 2025  
Commission number 1126044  
Member, Pennsylvania Association of Notaries

By: *Teresa Pastella*  
Teresa Pastella, Notary Public

This Power of Attorney is made and executed pursuant to and by authority of the following By-law and Authorizations of The Ohio Casualty Insurance Company, which is now in full force and effect reading as follows:

**ARTICLE IV – OFFICERS: Section 12. Power of Attorney.**  
Any officer or other official of the Corporation authorized for that purpose in writing by the Chairman or the President, and subject to such limitation as the Chairman or the President may prescribe, shall appoint such attorneys-in-fact, as may be necessary to act in behalf of the Corporation to make, execute, seal, acknowledge and deliver as surety any and all undertakings, bonds, recognizances and other surety obligations. Such attorneys-in-fact, subject to the limitations set forth in their respective powers of attorney, shall have full power to bind the Corporation by their signature and executed, such instruments shall be as binding as if signed by the President and attested to by the Secretary. Any power or authority granted to any representative or attorney-in-fact under the provisions of this article may be revoked at any time by the Board, the Chairman, the President or by the officer or officers granting such power or authority.

**Certificate of Designation** – The President of the Company, acting pursuant to the Bylaws of the Company, authorizes David M. Carey, Assistant Secretary to appoint such attorneys-in-fact as may be necessary to act on behalf of the Company to make, execute, seal, acknowledge and deliver as surety any and all undertakings, bonds, recognizances and other surety obligations.

**Authorization** – By unanimous consent of the Company's Board of Directors, the Company consents that facsimile or mechanically reproduced signature or electronic signatures of any assistant secretary of the Company or facsimile or mechanically reproduced or electronic seal of the Company, wherever appearing upon a certified copy of any power of attorney or bond issued by the Company in connection with surety bonds, shall be valid and binding upon the Company with the same force and effect as though manually affixed.

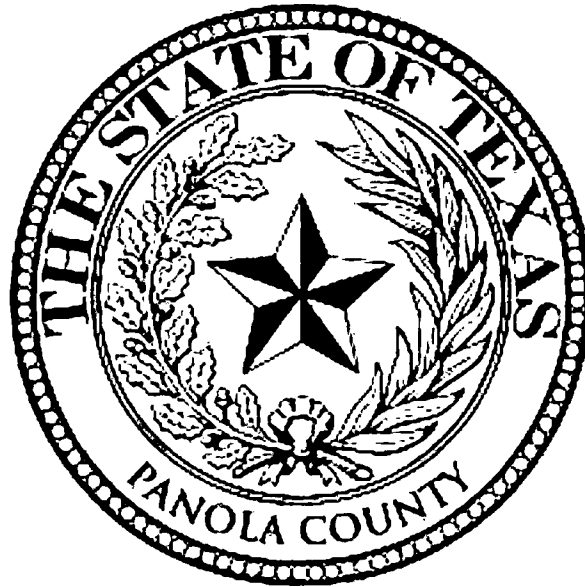
I, Renee C. Llewellyn, the undersigned, Assistant Secretary, of The Ohio Casualty Insurance Company do hereby certify that this power of attorney executed by said Company is in full force and effect and has not been revoked.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seals of said Company this 1st day of November, 2023.



By: *Renee C. Llewellyn*  
Renee C. Llewellyn, Assistant Secretary

*PANOLA COUNTY  
ELECTIONS  
INFORMATION SECURITY  
POLICY*





Contents

INTRODUCTION ..... 6

SECTION 1: IDENTIFY ..... 7

- POLICY 1: GOVERNANCE ..... 7
- POLICY 2: BUSINESS ENVIRONMENT ..... 8
- POLICY 3: SECURITY RISK ASSESSMENT AND MANAGEMENT STRATEGY..... 9
- POLICY 4: SUPPLY CHAIN RISK MANAGEMENT ..... 10
- POLICY 5: ASSET MANAGEMENT ..... 11

SECTION 2: PROTECT ..... 14

- POLICY 6: DATA SECURITY AND INFORMATION PROTECTION ..... 14
- POLICY 7: IDENTITY MANAGEMENT, AUTHENTICATION AND ACCESS CONTROL..... 17
- POLICY 8: ELECTION INFORMATION SYSTEM MAINTENANCE ..... 18
- POLICY 9: USE OF PROTECTIVE TECHNOLOGY ..... 19
- POLICY 10: INFORMATION SECURITY AWARENESS TRAINING ..... 20

SECTION 3: DETECT ..... 21

- POLICY 11: CONTINUOUS SECURITY MONITORING..... 21
- POLICY 12: DETECTING ANOMALIES AND EVENTS..... 22
- POLICY 13: ELECTION STAFF DETECTION PROCESSES ..... 23

SECTION 4 OBJECTIVE: RESPOND EFFECTIVELY TO ATTACKS..... 24

- POLICY 14: RESPONSE PLANNING ..... 24
- POLICY 15: ANALYSIS ..... 25
- POLICY 16: MITIGATION OF CYBERATTACKS..... 26
- POLICY 17: RESPONSE COMMUNICATIONS ..... 27
- POLICY 18: RESPONSE IMPROVEMENTS ..... 28

SECTION 5 OBJECTIVE: RECOVER..... 29

- POLICY 19: RECOVERY PLANNING ..... 29
- POLICY 20: RECOVERY IMPROVEMENTS ..... 30
- POLICY 21: RECOVERY COMMUNICATIONS..... 31

APPENDIX A: ROLES AND SECURITY RESPONSIBILITIES ..... 32

APPENDIX B: THREAT AND RISK MONITORING LOG..... 35



APPENDIX C: TECHNOLOGY ASSET INVENTORY, CLASSIFICATION, CHAIN OF CUSTODY AND CHANGE MANAGEMENT ..... 37

APPENDIX D: REMOVABLE MEDIA POLICY ..... 39

APPENDIX E: NETWORK TOPOLOGY DIAGRAM..... 41

APPENDIX F: DATA INVENTORY AND CLASSIFICATION ..... 43

APPENDIX G: ACCESS PERMISSIONS..... 44

## **CONFIDENTIAL INFORMATION WARNING**

This document contains information about the security of Panola County Elections 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 Panola County Elections Confidential, and cannot be reproduced, redistributed in any way, shape or form without prior written consent from Panola County Elections.

# INTRODUCTION

The Panola County Elections 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 Panola County Elections build 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 Panola 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 Panola County Elections.
- The Policy meets applicable federal, state and local laws in addition to Panola County Elections policies, regulations and contractual obligations.

# SECTION 1: IDENTIFY

---

## POLICY 1: GOVERNANCE

Panola County Elections 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 Loretta Mason as the election administrator 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.
- An up-to-date printed copy of the Election WISP is stored in a binder located 3<sup>rd</sup> floor election room. 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 Loretta Mason Election Administrator. They are documented and tracked using the Security Roles and Responsibilities Chart.

---

## POLICY 2: BUSINESS ENVIRONMENT

*Panola 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.

### MISSION STATEMENT

- *Provide the public with courteous, prompt and professional service*
- *Strive and work as a team with loyalty and respect for each other*
- *Strive to have accurate election totals*
- *To conduct fair and honest elections on all levels, from county, state and federal levels*
- *To conduct elections, certify the canvass and retain all official records.*

### CRITICAL OPERATIONS

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 23 DS200, 23 ballot boxes, 40 Express Vote and 23 ES&S pollbooks 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	<p>Servers storing voter and candidate information</p> <p>Election systems</p> <p>ePollbooks</p> <p>Website Server and/or Hosting Account</p> <p>Voter Registration System Account</p> <p>Encrypted Backup Hard Drive</p>	<ul style="list-style-type: none"> <li>• Physical Assets                             <ul style="list-style-type: none"> <li>○ Assets must be stored in a locked location</li> <li>○ A two-person verification record in an access log is required for entry to area</li> <li>○ Access is limited to authorized personnel only</li> <li>○ Written approval must be obtained before access to the area is granted</li> <li>○ Physical assets in offsite locations such as IT vendor facilities must be stored in a locked area with restricted and controlled access</li> </ul> </li> <li>• Software Assets                             <ul style="list-style-type: none"> <li>○ Access is limited to authorized personnel only with strict limitations on who receives administrator privileges</li> <li>○ Written approval is required before access credentials or administrator privileges will be granted</li> <li>○ Unique usernames must be used</li> <li>○ Credential sharing is strictly prohibited</li> <li>○ Strong passwords are required</li> <li>○ Multifactor authentication is required where possible</li> <li>○ On premise assets must be contained within the election network firewall</li> <li>○ Remote and Internet access is restricted</li> </ul> </li> </ul>

		<ul style="list-style-type: none"> <li>○ Continuous monitoring for suspicious activity is required</li> <li>○ Data must be backed up using encryption</li> <li>○ Chain of custody record is required</li> </ul>
<b>2</b>	<p>Employee desktops and laptops</p> <p>Mobile devices</p> <p>Productivity Software</p> <p>Social media accounts</p>	<ul style="list-style-type: none"> <li>• Physical Assets <ul style="list-style-type: none"> <li>○ Protect physical access to hardware assets by keeping them in a locked area when not in use</li> <li>○ Assignment log is required</li> <li>○ Limit area access to personnel or escorted visitors only</li> </ul> </li> <li>• Software Assets <ul style="list-style-type: none"> <li>○ Approval process not required, but access credentials should be assigned to personnel only</li> <li>○ Assign unique usernames and prohibit credential sharing</li> <li>○ Require strong passwords</li> <li>○ Require multifactor authentication where possible</li> <li>○ Keep the asset located behind election-specific firewall in the network</li> <li>○ Remote access via a Virtual Private Network permissible</li> <li>○ Monitor for suspicious activity</li> <li>○ Backup data using encryption</li> </ul> </li> </ul>
<b>3</b>	<p>Printers</p> <p>Copy Machines</p> <p>Fax machines</p>	<ul style="list-style-type: none"> <li>• Locked area not required, but advised</li> <li>• Require strong passwords if needed</li> <li>• Multifactor authentication not required</li> <li>• Monitor for suspicious activity</li> </ul>



## 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 flash drive that is not connected to the Internet or the election network and that is stored offsite Road and Bridge election room.
- 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 by using a formatted non network connected PC located upstairs 3<sup>rd</sup> floor election room 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
<b>Confidential</b>	
<p>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.</p>	<ul style="list-style-type: none"> <li>• Written Information Security Program</li> <li>• Election Information Security Policy</li> <li>• Election System Security Plan</li> <li>• Cybersecurity Incident Response Plan</li> <li>• Continuity of Operations Plan</li> <li>• Vendor Risk Management Policy</li> <li>• Vendor Risk Assessment Results</li> <li>• Election Security Assessment (ESA) Results</li> <li>• Employee and Poll Worker Personally Identifiable Information and Financial Data</li> <li>• Election Department Critical Infrastructure Information</li> <li>• Polling Location Technology Configuration</li> <li>• Passwords, Including Login Credentials for All Systems and Election Devices</li> <li>• Vulnerability Scan Data</li> <li>• Threat Monitoring and Cyber Intelligence Information</li> <li>• System Inventory Information</li> <li>• System Life Cycle Management Information</li> <li>• Security Incident Reports or Event Details</li> <li>• Protected Voter Registration Application Information including items Defined in Election Code 13.004 (c) including:                         <ul style="list-style-type: none"> <li>○ Social security number</li> <li>○ Texas Driver License or TX Personal Identification Card Number</li> <li>○ Indication that the applicant is interested in working as an election judge</li> <li>○ Residence address of federal or state judges and their spouses</li> <li>○ 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</li> <li>○ Residence address of applicants participating in the address confidentiality program</li> <li>○ Residence address of peace officers and other protected individuals under Texas Law.</li> </ul> </li> </ul>



	<ul style="list-style-type: none"> <li>○ Voter Registration Data Disclosing Criminal History or Voter Activity/Inactivity</li> <li>○ Voter Registration Application Source Codes</li> </ul> <p><i>*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</i></p>
<b>Sensitive</b>	
<p>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.</p>	<ul style="list-style-type: none"> <li>● Voter Registration Data Excluding Criminal History, Voter Activity/Inactivity and Data Defined as Confidential in Election Code 13.004 (c)</li> <li>● Candidate Application Instructions</li> <li>● Poll Worker Instructions</li> <li>● Election Process Handbook/Guide</li> <li>● Voter Instructions</li> <li>● Candidate Information</li> <li>● Draft Ballot and Proof Information</li> <li>● Preliminary Tabulation Results</li> <li>● Vendor Information Excluding Vendor Risk Assessment Results</li> <li>● Password Management Policies</li> <li>● Technology Storage and Transportation Details</li> <li>● Escalation Path and Communication Plans for Suspected Security Incidents or Events</li> <li>● Roles and Responsibility Definitions and Assignments</li> </ul>
<b>Internal Use</b>	
<p>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.</p>	<ul style="list-style-type: none"> <li>● Employee Handbooks</li> <li>● Security Awareness Training</li> <li>● Pollbook Technology Details</li> <li>● Background Check Processes</li> <li>● Vendor Information</li> <li>● Chain of Custody Documentation for Voting Systems and Ballots</li> <li>● Help Desk Instructions</li> <li>● Basic Facts About a Security Incident or Event <ul style="list-style-type: none"> <li>○ It Happened</li> <li>○ It Is Being Addressed Rapidly</li> <li>○ How It Impacts Voters</li> </ul> </li> </ul>
<b>Public Use</b>	
<p>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</p>	<ul style="list-style-type: none"> <li>● Election News and Announcements</li> <li>● Job Announcements</li> <li>● Election System and Voting Equipment Types</li> <li>● Voting System Type</li> <li>● Poll Locations</li> </ul>

declared public knowledge by someone with the proper authorization and should not be used or disclosed without approval.	<ul style="list-style-type: none"><li>• Election Schedules</li><li>• Ballot Information</li><li>• Tabulation Results</li><li>• Official Domain URLs</li></ul>
--	---

---

## 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 Loretta Mason, Elections 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 Loretta Mason, Elections 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 Loretta Mason, Elections Administrator 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.
- *Loretta Mason Elections Administrator* must lead frequent discussions about security practices with the team 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
- Monitoring activity must be conducted to detect unauthorized:
  - Connections
  - Devices
  - Software
  - Personnel

---

## 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 Loretta Mason, 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. Staff must notify Barry Tate IT specialist of a high volume of blocked attack alerts.

## 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 described 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 Loretta Mason, Elections Administrator, Barry Tate, IT specialist and Bryan Murff, Emergency Management Coordinator 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 Elections 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 Loretta Mason, Elections Administrator.

## 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 Loretta Mason, Elections Administrator.



---

## 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 Loretta Mason, Elections Administrator.

---

## 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	<ul style="list-style-type: none"> <li>• Ensure the Election WISP is accessible only to election staff and all employees know where to find it and how to access it.</li> <li>• Ensure the Election WISP is approved and authorized by leadership.</li> <li>• Coordinate Election WISP reviews and updates in December after an election and in June after a legislative session.</li> <li>• If new cyber threats are identified, ensure that Election WISP policies and plans are updated with practices that protect against them.</li> <li>• Notify IT or cybersecurity resources of any reports from staff of suspicious activity or events that could indicate an active attack incident.</li> <li>• 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.</li> <li>• Notify the Texas Department of Information Resources if the activity is determined to be a true threat.</li> <li>• Conduct an annual review of changes to operations and if the changes introduce new opportunities for cyberattacks.</li> <li>• Ensure that the most current version of the Election WISP is covered in the mandatory annual employee security awareness training curriculum.</li> </ul>
All Election Staff	<ul style="list-style-type: none"> <li>• Remain vigilant for indicators of a cyberattack.</li> <li>• 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.</li> <li>• Annually participate in security awareness training and Table-Top Exercises.</li> <li>• Know where to find the Election WISP.</li> <li>• 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.</li> <li>• Follow news about security threats and cybercrime trends and understand their potential impact to your elections.</li> </ul>

Supply Manager	<ul style="list-style-type: none"> <li>• Ensure that vendor contracts include the requirement to follow the Election Information Security Policy and the Vendor Risk Management Policy.</li> <li>• Ask vendors to provide security assessment results that include their security policies, plans and practices and store them with the vendor contract.</li> <li>• 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.</li> </ul>
Office Manager	<ul style="list-style-type: none"> <li>• Maintain an up-to-date inventory of assets.</li> <li>• Require that visitors to the facility sign into a visitor log book, have name tags, and are escorted by staff.</li> <li>• Ensure that facilities are locked, and surveillance camera video is properly recorded and stored according to retention policies.</li> </ul>
IT Manager	<ul style="list-style-type: none"> <li>• Implement the data security requirements in the Security Best Practice Guidelines, Election Information Security Policy and the Election Systems Security Policy.</li> <li>• Monitor cyber intelligence feeds from MS-ISAC/EI-ISAC and the media for cyber threat trends that could impact elections and require defense adjustments.</li> </ul>
Voter Registrar	<ul style="list-style-type: none"> <li>• Adhere to the Election Information Security Policy and the Elections Systems Security Policy.</li> <li>• Report suspicious activity to the Election Administrator who will immediately notify the appropriate entities to determine if the activity indicates an incident.</li> <li>• 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.</li> <li>• Communicate voter registration process changes to the Election Administrator and request that the changes be incorporated into Election WISP if needed.</li> </ul>




APPENDIX B: THREAT AND RISK MONITORING LOG

MONITORING FREQUENCY: WEEKLY		ASSIGNED TO: IT Manager			
MONITORING SOURCES: MS-ISAC/EI-ISAC ALERTS, MEDIA CHANNELS		REPORT SIGNIFICANT FINDINGS TO: Elections Administrator			
POLICY UPDATE FREQUENCY: TWICE/YEAR OR WHEN SIGNIFICANT THREATS EMERGE		POLICY UPDATE APPROVAL BY: Election Administrator			
Identified Risk	Potential Impact (including operations, assets and individuals)	Security Measures Implemented	Policy Update Section and Date If Required	Logged By, Date	
Tornado/flood	Likely would have to change polling locations	Work with back up polling places to get permission to use those polling places in case of an emergency			
Ice/Snow storm	Safety of workers and voters	Work with polling locations to open later and inform SOS of the situation			
Illness/Accident	Loss of worker Loss of productivity	Work withing our office to get help to replace worker			
EI-ISAC	Exploitation of Systems Vulnerabilities	Lack of information Lack of support			





APPENDIX C: TECHNOLOGY ASSET INVENTORY, CLASSIFICATION, CHAIN OF CUSTODY AND CHANGE MANAGEMENT

TECHNOLOGY ASSET INVENTORY, CLASSIFICATION, CHAIN OF CUSTODY, CHANGE MANAGEMENT LOG											
ASSET GROUP: OFFICE EQUIPMENT											
INVENTORY											
Asset Model, Type and Serial or Product Number, I have attached a list of serial numbers	Connected to Network?	Confidential and Sensitive Data Removed Before Moving Offsite?									
23 Ballot Boxes	Yes	Yes									
23 DS 200	No	N/A									
40 Express Votes	No	Yes									
23 ES&S Poll books	No	N/A									

Where/ Who	Computer	Keyboard	Mouse	Label Printer	Scanner	Laptop	Laptop Keyboard	Laptop Mouse	Fax	Printers	Phone Earpiece	Other
Voter Registration												
Voter Registrar	H4TG5169Q6XF	FCC ID: BCGA2520	FCC ID:BCGA1657	1750110-2A92655	C6UH029519	C02GCOMFML87	FCC ID: BCGA1644	FCC ID: BCGA1657	U63274G2J17933	Xerox: 3TX399224	25N8RL	Shredder: UNU-38251
Deputy Voter Registrar	H4TG11PPQ6W1	FCC ID: BCGA2520	FCC ID:BCGA1657	1750110-2091624	C6UH029524	C02GCONNML87	FCC ID: BCGA2449	FCC ID: BCGA1657		Xerox: 5AV420102	25N8RM	Paper Folder: 20F1D077
Third Computer	C02Z338NJV3P	FCC ID: BCGA1644	FCC ID: BCGA1657							HP: PHBH50112	25N8FO	
Road & Bridge												
Ballot Boxes	No Serial Numbers											
Third Floor	DS200	Black Case	ExpressVote	Tablets	Computer	Printer	Phone	Flash Drives	Cell Phones			
Pct 1	DS0322370229	231217	EV0222310363	2541212551	HK8NPR3	U64285A2N507663	A18996BA100934		DX312ATPODXP			
Pct 2	DS0322370169	230921	EV022310121	2514212551					DX312CAMODXP			
Pct 3	DS0322370049	230935	EV0220410139	24749212451								
Pct 5	DS0322370389	230821	EV0222310382	2482512551								
Pct 7	DS0322370364	231178	EV0222310074	2569612551								
Pct 8	DS0322370119	231228	EV0222310220	2417712551								
Pct 9	DS0322370430	231105	EV0222310118	2557212551								
Pct 10	DS0322370207	231269	EV0222310103	585312551								
Pct 12	DS0322370418	230863	EV0222310133	2513312551								
Pct 13	DS0322370173	231413	EV0222310087	940112551								
Pct 14	DS0322370427	231088	EV0222310282	2367312551								
Pct 18	DS0322970179	231279	EV0222310122	2211112551								
Pct 19	DS0322370429	230911	EV0222310102	25082412451								
Pct 20	DS033270133	231063	EV0222310100	2499412551								
Pct 22	DS0322370219	231032	EV0222310101	2515112551								
Pct 26	DS0322370416	231541	EV022310109	639312551								
Pct 27	DS0322370162	231188	EV0222310232	2140712551								
Pct 28	DS0322370365	231567	EV0222310130	245612451								
Pct 29	DS0322370148	231180	EV0222310140	2320712551								
Extra 1	DS0322370417	202384	EV0220410060	24228312451								
Extra 2	DS0322370454	216305	EV0222310096	2145212551								
Extra 3	DS0322370454	231197	EV0222310139	2487712551								
Early Voting	DS0322370166	231111	EV0222310242	2588512551								
		216868	EV0222310267									
		231505	EV022310068									
		15509	EV0222310359									
		231237	EV0222310089									
			EV0222310123									
			EV022310212									
			EV022310311									
			EV0222310309									
			EV022310128									
			EV0222310091									
			EV0222310141									
			EV0222310041									
			EV022310127									
			EV0222310080									
			EV0222310287									
			EV0222310136									
			EV0222310132									

## **Overview**

Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organizations. As an Election Authority, it is imperative that every removable media device be tightly controlled and properly used in order to protect the integrity of the election process.

### **2.0 Purpose**

The purpose of this policy is to minimize the risk of loss or exposure of sensitive election information and to reduce the risk of acquiring malware infections on computers. Any questions or comments about this policy should be directed to Loretta Mason Election Administrator.

### **3.0 Scope**

This policy covers all removable media that contains election data or that is connected to the secure network.

### **4.0 Policy**

Staff may only use specifically approved removable media devices on any system or network related to an election or to any election process. Each media device must be properly noted in the inventory logs and an IT administrator must make changes to the Election Secure Network to allow computers to access the removable media device.

Any other removable media used must be approved by leadership and requires the use of an encrypted USB device that uses FIPS 140-2 approved encryption levels. The following devices are specifically approved for use:

ES&S USB Flash drive

Apple Computers, Serial #s H4TGS169Q6XF, H4TG11PPQW1, CO22338NJV3P. Apple laptops Serial #s CO2GCOMFML87, CO2GCDNNML87.

No exceptions to this policy are allowed.

### **5.0 Enforcement**

Anyone found to have violated this policy may be subject to disciplinary action, up to and including suspension of access to technology resources or termination of employment.

### **6.0 Definitions**

#### **Removable Media**

Removable media is defined as devices or media that is readable and/or writable by the end user and are able to be moved from computer to computer without modification to the computer. This includes flash memory devices such as thumb drives, SD cards, cameras, MP3 players and PDAs; removable hard drives (including hard drive-based MP3 players); optical disks such as CD and DVD disks; floppy disks and software disks.

#### **Encryption**

Encryption is a procedure used to convert data from its original form to a format that is unreadable and/or unusable to anyone without the tools/information needed to reverse the encryption process. Encryption is provided in various forms, some of which are more secure than others. In order to ensure a suitable level of encryption, users are required to only use devices that are approved by the federal government with a FIPS 140-2 level of encryption.

#### **Malware**



Malware is defined as software of malicious intent/impact such as viruses, worms, and spyware.

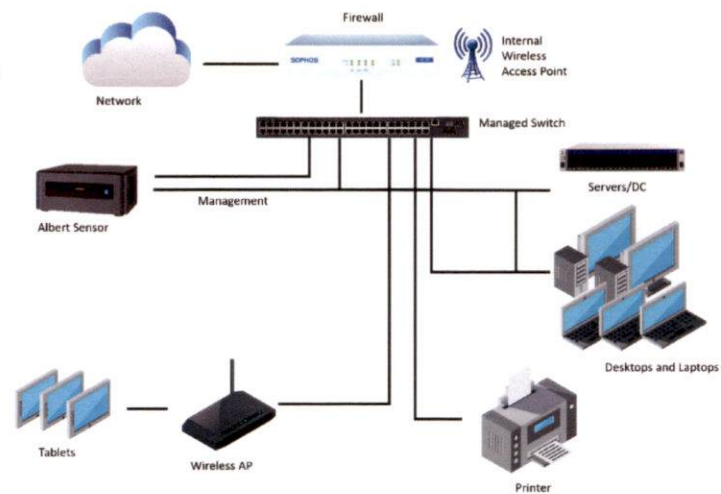
### Sensitive Information

Sensitive information is defined as information which, if made available to unauthorized persons, may adversely affect the election process. Examples include, but are not limited to, voter data, election processes, unreleased election data, personal identifiers and financial information.

## APPENDIX E: NETWORK TOPOLOGY DIAGRAM

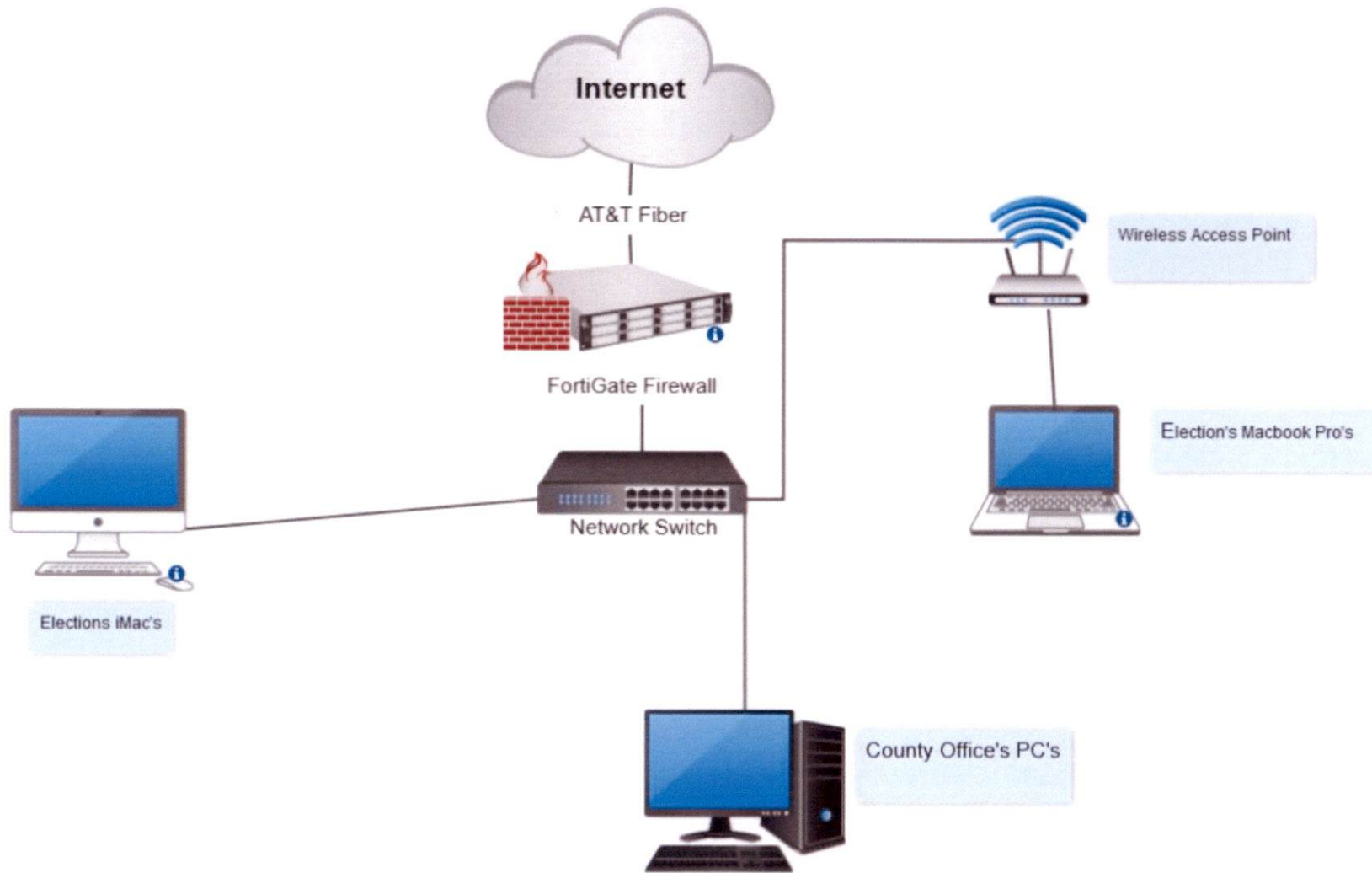
A network topology diagram doesn't have to be complex. The main objective is to create a visual representation of how each system connects to other systems. This can be simply drawn out on a piece of paper, or it can be created using PowerPoint. This diagram was created using PowerPoint and icon graphics.

Example  
Network  
Topology  
Diagram





# Panola County Network Layout



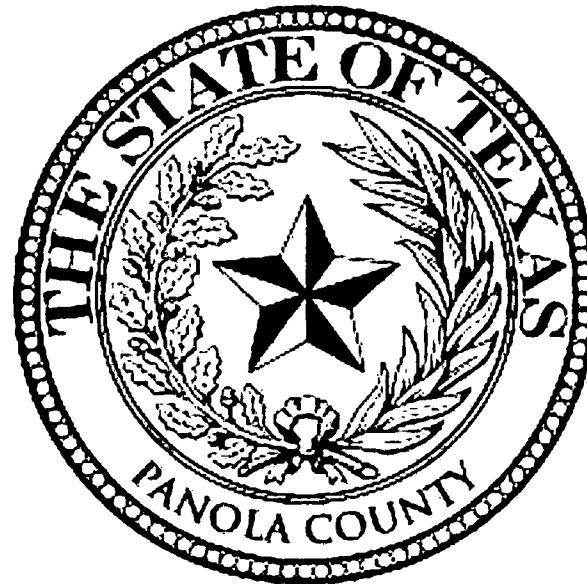
APPENDIX F: DATA INVENTORY AND CLASSIFICATION

Critical Operation Support	Data Classification	Data Type	Location	Connected to Network	Access Permission
Voter Registration	Confidential	Voter Personal Identifying Information (PII)	TEAM	Yes	Voter Registrar, Election Administrator, Poll Workers
Elections Administrator	Confidential	Run and maintain election data and the outcome of elections	TEAM/Computer	Yes	Voter Registrar, Elections Administrator,
Equipment	Confidential	local	3 <sup>rd</sup> floor election room	No	Staff Members
Ballot by mail	Confidential/Sensitive	Local	TEAM	Yes	Stall Members
Train VDR		Local	My computer	Yes	Elections Administrator
Train Judges, Alt.Judges, Clerks		Local	My computer	Yes	Elections Administrator/Staff

APPENDIX G: ACCESS PERMISSIONS

Asset	User	Admin	User and Admin
TEAM Voter Registration System	Poll workers Election Administrator Office Manager	<b>Elections Administrator</b>	Registrar
Website	Election Administrator/Staff/IT Director	IT Director	Kelsey Gates/Communications Director
ePollbooks	Poll workers	ES&S	Election Administrator
Employee Laptops	Employee	EA/IT Director	Employees
Firewall	IT Director	Administrator	IT Director
Facebook/Social Media Channels	Deputy Election Administrator/Deputy Voter Registrar	Elections Administrator	Elections Administrator/Deputy Elections Administrator
ES&S Portal	Elections Administrator	ES&S	Elections Administrator/ES&S


*PANOLA COUNTY ELECTIONS  
CONTINUITY OF OPERATIONS PLAN  
FOR ELECTIONS*





PLAN REVIEW LOG

PLAN ADOPTED DATE						
Drafted By		Loretta Mason		Signature		Date
Approved By		Rodger McLane		Signature		Date
REVIEW AND REVISION LOG						
REVIEW SCHEDULE		General Election Years: December after elections			Legislative Session Years: July after SOS Law Conference	
Review Date	If Revised, Revision Date	Revision Description (Or Specify "No Revisions" If None Made)	Drafted By: Title	Signature, Date	Approved By: Title	Signature, Date


## Contents

INTRODUCTION ..... 13

    PURPOSE ..... 13

    ASSUMPTIONS..... 14

CONTINUITY OF OPERATIONS FOR ESSENTIAL ELECTION FUNCTIONS ..... 16

    ELECTION STAFF SUPPORT ..... 16

        Table 1: Election Staff Support Alternative Technology and Data Plan..... 19

    ELECTION MANAGEMENT ..... 22

        Table 2: Election Management Alternative Technology and Data Plan ..... 25

    VOTER REGISTRATION ..... 28

        Table 3: Voter Registration Alternative Technology and Data Plan ..... 30

    BALLOT CREATION AND DISTRIBUTION ..... 33

        Table 4: Ballot Creation and Distribution Alternative Technology and Data Plan..... 35

    ePOLLBOOK AND VOTER CHECK-IN AND QUALIFICATION ..... 37

        Table 5: ePollbook/Voter Check-In and Qualification Alternative Technology and Data Plan..... 39

    VOTE CASTING AND CAPTURE..... 42

Table 6: Vote Casting and Capture Alternative Technology and Data Plan..... 44

VOTE TABULATION..... 47

Table 7: Vote Tabulation Alternative Technology and Data Plan..... 49

ELECTION NIGHT REPORTING..... 52

Table 8: Election Night Reporting Alternative Technology and Data Plan ..... 54

APPENDIX A: ELECTION CONTINUITY OF OPERATIONS CONTACT LIST ..... 56

APPENDIX B: EARLY VOTING AND ELECTION DAY WORKER CONTACT LIST ..... 58

APPENDIX C: RESPONSIBILITY SUCCESSION PLAN ..... 62

APPENDIX D: JOB RESPONSIBILITIES AND TASKS GUIDE ..... 66

APPENDIX E: ALTERNATE UTILITIES AND FACILITIES PLAN ..... 66

APPENDIX F: RELOCATION CHECKLIST..... 71

## INTRODUCTION

### PURPOSE

The purpose of the Continuity of Operations Plan (COOP) is to define a step-by-step process for keeping election functions operational during disruptions such as those caused by cyberattacks or other disaster events. The critical nature of elections makes it imperative that the Election Authority maintains a current version of this plan and that the plan is reviewed and updated on a regular basis. As a crucial element of the Election Written Information Security Program (WISP), the COOP directs staff on how to ensure an election can be held without delay or disruption even under negative circumstances.

The COOP is aligned to eight main election function areas including staff support, election management, voter registration, ballot creation, voter check-in, vote casting and capture, vote tabulation, and results reporting. This alignment ensures that plans for continued operation are in place to accommodate the potential impact a cyberattack or other disaster event could have on each function.



## ASSUMPTIONS

The Continuity of Operations Plan (COOP) is based on several assumptions related to the nature of the incident and the Election Authority's security awareness and preparedness.

The plan assumes that a cyberattack or disaster event has resulted in one or more of the following circumstances:

- Internet or phone access is no longer available
- Network is down and not accessible
- Election voting equipment is not operational
- ePollbooks are not operational
- Tabulation machines are not operational
- Critical staff members are not able to perform their duties
- Essential computers are compromised and can't be used
- Critical applications are compromised and can't be used
- Election administration main office is not usable
- One or more polling locations is not usable

The COOP also assumes that:

- The election team has complied with the requirements of the Election Information Security Policy, particularly:
  - Maintaining a frequently updated encrypted external hard drive with backups of critical data Road & Bridge election room.

- Maintaining an inventory of all essential technology and equipment
- Maintaining a current diagram of the network
- Adhering to the Election Data Classification System in the Election Information Security Policy to ensure that critical information is protected and backed up
- A Cybersecurity Incident Response Plan (IRP) is in place and the team is familiar with it. The IRP defines:
  - What constitutes a cyberattack incident and when to activate the Security Incident Response Plan
  - The members of the incident response team and their roles during an incident
  - An escalation path for notifying the response team and the appropriate resources
  - A communication plan that is aligned to the data handling criteria specified in the Election Data Classification System
- The following resources and information needed to support the COOP have been identified or created and assembled in a series of appendices listed here:
  - Election Continuity of Operations Contact List (Appendix A)
  - Early Voting and Election Day Worker Contact List (Appendix B)
  - Responsibility Succession Plan (Appendix C) and each next-in-line designee has been assigned login credentials for critical systems or applications
  - Job Responsibilities and Task Guide (Appendix D) for individuals with responsibility for critical business functions
  - Alternate Utilities and Facilities Plan (Appendix E)
  - Relocation Checklist (Appendix F)

## CONTINUITY OF OPERATIONS FOR ESSENTIAL ELECTION FUNCTIONS

### ELECTION STAFF SUPPORT

This section references the underlying processes and technologies that enable the Election Authority's business operations.

- The Election Administrator is responsible for ensuring that election staff have the resources needed for continuity of business operations.
- If the Elections Administrator, Loretta Mason is not available, refer to the Responsibility Succession Plan (Appendix C) and contact the next-in-line designee.
  - The Elections Administrator, Loretta Mason, is responsible for ensuring that the next-in-line designee has the required login credentials and the appropriate level of access permissions needed if the next-in-line designee must take over the role.
- Next-in-line designees must refer to the Job Responsibilities and Tasks Guide (Appendix D) and follow the instructions for assuming the responsibilities of the role.
  - These documents are stored with the Election Written Information Security Program (WISP) in an electronic format backed up to two encrypted external hard drives, one stored securely onsite in the 3<sup>rd</sup> floor election room and one stored offsite at the Road & Bridge Election Room. The documents are also maintained in a paper format in the Election WISP binder stored in the 3<sup>rd</sup> floor election room. Refer to Table 1: Election Staff Support Alternative Technology and Data Plan for information about how to access the backups of the Job Responsibilities and Tasks Guide, if needed.
- If regular communication capabilities such as office phone or email are lost, communication capabilities must be maintained via call and text using cell phones.

- Refer to the Election Continuity of Operations Contact List (Appendix A) to find mobile phone contact information.
- If any office systems related to managing elections are compromised or damaged, the *Election Administrator* is responsible for implementing alternate technology and data as outlined in Table 1: Election Staff Support Alternative Technology and Data Plan with support from our IT specialist Barry Tate.
  - These systems include:
    - Staff computers
    - Office productivity software
    - Network connectivity
    - Internet access
    - Email functionality
    - Phone systems
- If data has been lost or access to data is unavailable, retrieve the backups of the data needed to support the election team's functions.
  - Two copies of electronic, encrypted hard drive with data backups are regularly updated once per month and stored offline. One is stored 3<sup>rd</sup> floor election room and Road & Bridge election room.
  - When using the backed-up data, continue to follow data management policies according to the Election Data Classification System in the Election Information Security Policy.
    - This data includes:
      - Business operation plans and budgets
      - Human Resources records

- Documented employee job functions with access credentials
  - Contact lists
  - Election Written Information Security Program (WISP), which includes:
    - Election Information Security Policy
    - Security Incident Response Plan
    - Election System Security Plan
    - Election Vendor Risk Management Policy
    - This Continuity of Operations Plan
- If the Election Office is not usable or power is not available for extended time periods, the Expo Hall located on ballfield drive will be used as the early voting location.
- Refer to the Alternate Utilities and Facilities Plan (Appendix E) for details on when and how to relocate if necessary.
  - If relocation is needed, refer to the Relocation Checklist (Appendix F), coordinate the collection and transportation of needed items, and set up at the alternate site.
- The Elections Administrator, Loretta Mason must contact the insurance company that holds the cyber incident and disaster insurance policy to arrange coverage for the cost of replacing business operations technology lost to damaging events, if applicable. Refer to the Election Continuity of Operations Contact List (Appendix A) for contact information.



Table 1: Election Staff Support Alternative Technology and Data Plan

WHAT IS COMPROMISED	ALTERNATIVE	LOCATION	HOW TO ACCESS IT	ROLE WITH ACCESS OR RESPONSIBILITY TO TAKE ACTION			
				PRIMARY	DESK PHONE	NEXT-IN-LINE	DESK PHONE
Computer Needed for Essential Functions at Loretta's desk	Laptop	Located in my office behind my desk	N/A	Election Administrator	903-754-7275	Deputy EA/VR	903-754-7924
Computer Needed for Essential Functions at Kelsey's desk	Laptop	located in Kelsey's office by the printers	N/A	Election Administrator	903-754-7275	Deputy EA/VR	903-754-7924
Internet Access	Mobile Hotspot Device 1	Locked 3 <sup>rd</sup> floor election room	Loretta or Kelsey has keys and knows where	Election Administrator	903-754-7275	Deputy EA/VR	903-754-7924

			backup is located				
Internet Access	Mobile Hotspot Device 2	Locked 3 <sup>rd</sup> floor election room	Loretta or Kelsey has keys and knows where backup is located	Election Administrator	903-754-7275	Deputy EA/VR	903-754-7924
Email Functionality	Cell Phone Numbers for Calls and Texts	Refer to Election Continuity of Operations Contact List	N/A	Election Administrator	903-754-7275	Deputy EA/VR	903-754-7924
Data Needed for Essential Business Operations	Data Backup on Encrypted Hard Drive 1	Locked 3 <sup>rd</sup> floor election room	Loretta & Kelsey have keys to this room	Election Administrator	903-754-7275	Deputy EA/VR	903-754-7924

# PLAN

Data Needed for Essential Business Operations	Data Backup Encrypted Hard Drive 2	Road & Bridge Election Room	Loretta & Kelsey have keys to this room	Election Administrator	903-754-7275	Deputy EA/VR	903 754-7924
Primary Staff Member(s) Responsible for Staff Support Functions	Next-in-Line Designee Follows Documented Job Duties	Documents in Election WISP binder in locked 2 <sup>nd</sup> floor storage closet, or on backup hard drive	Key to 3 <sup>rd</sup> floor election room, Road & Bridge Election room and approval	Election Administrator	903-754-7275	Deputy EA/VR	903-754-7924Lap

## ELECTION MANAGEMENT

This section references the underlying technologies and processes that enable the Election Authority's election operations.

- If election systems are compromised or damaged, the Election Administrator is responsible for implementing alternate election systems with support from the Deputy VR/Deputy EA, Kelsey Gates and election equipment vendors.
  - These systems and resources include:
    - Access to Secretary of State resources
    - Voting machines
    - Tabulation machines
    - ePollbooks
    - Website and social media channels
  - Refer to Table 2: Election Management Alternative Technology and Data Plan for information on resources available for use if any of these systems is compromised.
- Refer to the Responsibility Succession Plan (Appendix C) and contact the next-in-line designee if the Election Administrator or Deputy VR/EA is not available.
  - The Elections Administrator, Loretta Mason and other personnel with critical election management duties are responsible for ensuring that the next-in-line designee has the required login credentials and the appropriate level of access permissions needed if the next-in-line designee must take over the role.
- Next-in-line designees must refer to the Job Responsibilities and Tasks Guide (Appendix D) and follow the instructions for assuming the responsibilities of the role.

- These documents are stored with the Election Written Information Security Program (WISP) in an electronic format backed up to two encrypted external hard drives, one stored securely onsite on the 3<sup>rd</sup> floor election room
- and one stored offsite in at the road & bridge election room. The documents will also be maintained in a paper format in the Election WISP binder stored in the locked 2<sup>nd</sup> floor storage closet.
- Refer to Table 2: Election Management Alternative Technology and Data Plan for information on how to access the backups of Job Responsibilities and Tasks Guides if needed.
- Refer to the Early Voting and Election Day Worker Contact List (Appendix B) for contact information and engage the Early Voting and Election Day Worker Coordinator who will serve as the single point of contact for communicating emergency and/or alternative procedure instructions and for receiving information from early voting and election day workers in the event of a cyberattack or disaster event.
- If regular communication capabilities such as office phone or email are lost, staff members and early voting and election day workers must use cell phones to maintain communication capabilities via call and text. Refer to the Election Continuity of Operations Contact List (Appendix A) and Early Voting and Election Day Worker Contact List (Appendix B) to find mobile phone contact information.
- If data needed to support election management is lost, or access to the data is unavailable, retrieve the backups of the needed data.
  - This data includes:
    - Voter registration data
    - Candidate information
    - Polling location details



- Early Voting and Election Day Worker Contact List (Appendix B)
- Ballot designs and source files
- Two copies of the encrypted external hard drives with data backups are regularly updated once per month and stored offline. One is stored 3<sup>rd</sup> floor election room and the other offsite at road & bridge election room.
- When using the backed-up data, continue to follow data management policies according to the Election Data Classification System in the Election Information Security Policy.
- If the polling locations are not usable or power is not available for extended time periods, move polling operations to the facility near the polling location designated as the backup location in the Alternate Utilities and Facilities Plan (Appendix E). Visible signs must be posted at the original polling location directing voters to the alternate location.
- Refer to the Alternate Utilities and Facilities Plan (Appendix E) for details on alternate facilities for each polling location and for details on when and how to relocate if necessary.
- If relocation is needed, refer to the Relocation Checklist (Appendix F) to make sure all needed items are transported and set up at the alternate site.
- The Elections Administrator, Loretta Mason must contact the insurance company that holds the cyber incident and disaster insurance policy to arrange coverage for the cost of replacing business operations technology lost to damaging events, if applicable. Refer to the Election Continuity of Operations Contact List (Appendix A) for contact information.

Table 2: Election Management Alternative Technology and Data Plan

WHAT IS COMPROMISED	ALTERNATIVE	LOCATION	HOW TO ACCESS IT	ROLE WITH ACCESS OR RESPONSIBILITY TO TAKE ACTION			
				PRIMARY	DESK PHONE	NEXT-IN-LINE	DESK PHONE
ERM Computer Needed for Essential Election Management Functions	ES&S would have to overnight a backup	N/A	N/A	Election Administrator	903-754-7275	Deputy EA/VR	903-754-7924
TEAM system	Laptop #1	Located in Loretta's office behind my desk	N/A	Election Administrator	903-754-7275	Deputy EA/VR	903-754-7275
Internet Access	Mobile Hotspot Device 1	Locked 3 <sup>rd</sup> floor	Loretta & Kelsey have	Election Administrator	903-754-7275	Deputy EA/VR	903-754-7275

		election room	keys to this room				
DS200, Express Vote & EPollbooks	Backup equipment	Locked 3 <sup>rd</sup> floor election room	Loretta & Kelsey have keys to this room	Election Administrator	903-754-7275	Deputy EA/VR	903-754-7924
Email Functionality	Use Cell Phones or Calls and Texts	Refer to the Election Continuity of Operations Contact List	N/A	Election Administrator	903-754-7275	Deputy EA/VR	903-754-7924
Data Needed for Essential Election Management	Data Backup on Encrypted Hard Drive 1	Locked 3 <sup>rd</sup> floor election room & Road & Bridge election room	Loretta & Kelsey have keys	Election Administrator	903 754 7275	Deputy EA/VR	903 754-7924

# PLAN

Primary Staff Member(s) Responsible for Election Management	Next-in-Line Designee Follows Documented Job Duties	Documents in Election WISP binder in locked 3 <sup>rd</sup> floor election room	Loretta & Kelsey have keys to that room	Election Administrator	903-754-7275	Deputy EA/VR	903-9754-7924
---	---	---	---	------------------------	--------------	--------------	---------------

## VOTER REGISTRATION

This section references the underlying technologies and processes that enable the County Election Department to register voters, validate identities, and confirm voter eligibility before, during and after an election.

- The Elections Administrator, Loretta Mason is responsible for voter registration functions, ensuring records are accurately entered into the electronic systems, securely retaining paper copies, and programming ePollbooks with support from the Elections Administrator, Loretta Mason and election system vendors.
  - These systems and resources include:
    - Access to the State Voter Registration System
    - ePollbooks
  - Refer to Table 3: Voter Registration Alternative Technology and Data Plan for information on technology and data sources that should be used if any of these resources is compromised.
- Refer to the Responsibility Succession Plan (Appendix C) to find who should be contacted if the Elections Administrator, Loretta Mason is not available.
  - The Elections Administrator, Loretta Mason is responsible for ensuring that the next-in-line designee has the required login credentials and the appropriate level of access permissions needed if the next-in-line designee must take over the role. The Elections Administrator, Loretta Mason must also ensure that the next-in-line designee understands the voter registration process and records retention requirements.
- Next-in-line designees must refer to the Job Responsibilities and Tasks Guide (Appendix D) and follow the instructions for assuming the responsibilities of the role.

- These documents are stored with the Election Written Information Security Program (WISP) in an electronic format backed up to two encrypted external hard drives, one stored securely onsite in the 3<sup>rd</sup> floor election room\_ and one stored offsite in road & bridge election room. The documents will also be maintained in a paper format in the Election WISP binder stored in the 3<sup>rd</sup> floor election room \_
- Refer to Table 3: Voter Registration Alternative Technology and Data Plan for information on how to access the backups of election technology and supporting systems, if needed.
- If data needed to support voter registration is lost, or if access to the data is unavailable, retrieve the backups of the needed data. This data includes:
  - Voter registration data including back up electronic or paper lists of registered voters
  - Instructions for registering to vote
  - Processes for various registration and renewal methods.
  - Documented voter registration-related job functions
- Two copies of the encrypted external hard drives with data backups are regularly updated monthly and stored offline. One is stored 3<sup>rd</sup> floor election room and offsite at the road & bridge election room\_
- When using the backed-up data, continue to follow data management policies according to the Election Data Classification System in the Election Information Security Policy.



Table 3: Voter Registration Alternative Technology and Data Plan

WHAT IS COMPROMISED	ALTERNATIVE	LOCATION	HOW TO ACCESS IT	ROLE WITH ACCESS OR RESPONSIBILITY TO TAKE ACTION			
				PRIMARY	DESK PHONE	NEXT IN-LINE	DESK PHONE
Computer Needed for Voter Registration Functions	Laptop #1	Behind Loretta's desk	N/A	Voter Registrar	903-754-7275	Deputy EA/VR	903-754-7924
Computer Needed for Voter Register Functions	Laptop #2	Kelsey's office on her desk by printers	N/A	Voter Registrar	903-754-7275	Deputy EA/VR	903-754-7924
Internet Access to Voter Registration System	Mobile Hotspot Device 1	Locked in the 3 <sup>rd</sup> floor election room	Loretta & Kelsey have keys to this room	Voter Registrar	903-754-7275	Deputy EA/VR	903-754-7924

# PLAN

Internet Access to Voter Registration System	Mobile Hotspot Device 2	Locked in the 3 <sup>rd</sup> floor election room	Loretta & Kelsey have keys to this room	Voter Registrar	903-754-7275	Deputy EA/VR	903-754-7924
Primary Staff Member(s) Responsible for Voter Registration	Next-in-Line Designee Follows Documented Job Duties	Documents in Election WISP binder in locked 2 <sup>nd</sup> floor storage closet, or on backup hard drive	Loretta & Kelsey have keys to this room	Voter Registrar	903-754-7275	Deputy EA/VR	903-754-7924
Voter Registration Data	Voter Registration Data Backup on Encrypted Hard Drive 1	Locked 3 <sup>rd</sup> floor election room	Loretta & kelsey have keys to this room	Voter Registrar	903-754-7275	Deputy EA/VR	903-754-7924
Electronic Access to Voter	PDF of OLRV	Locked in the 3 <sup>rd</sup> floor	Loretta & kelsey have	Voter Registrar	903-754-7275	Deputy EA/VR	903-754-7924

Registration Data	And or flash drive	election room	keys to this room				
----------------------	-----------------------	------------------	----------------------	--	--	--	--

## BALLOT CREATION AND DISTRIBUTION

This section references the underlying technologies and processes that enable the County Election Department to create ballots and program voting machines.

- The Elections Administrator is responsible for overseeing ballot creation and ensuring that ballots are accurately programmed into voting machines with support from the Elections Administrator, Loretta Mason and election system vendors.
  - These systems and resources include:
    - Design software
    - Voting machines
  - Refer to Table 4: Ballot Creation and Distribution Alternative Technology and Data Plan for information about technology and data sources that should be used if any of these resources is compromised.
- Refer to the Responsibility Succession Plan (Appendix C) to find who should be contacted if the Election Coordinator is not available.
  - The Elections Administrator is responsible for ensuring that the next-in-line designee has the required login credentials and the appropriate level of access permissions needed if the next-in-line designee must take over the role. The Elections Administrator must also ensure that the next-in-line designee understands the ballot creation and distribution process.
- Next-in-line designees must refer to the Job Responsibilities and Tasks Guide (Appendix D) and follow the instructions for assuming the responsibilities of the role.
  - These documents are stored with the Election Written Information Security Program (WISP) in an electronic format backed up to two encrypted external hard drives, one stored securely onsite in the 3<sup>rd</sup> floor election room\_and one

stored offsite at road & bridge election room. The documents will also be maintained in a paper format in the Election WISP binder stored on the 3<sup>rd</sup> floor election room.

- Refer to Table 4: Ballot Creation and Distribution Alternative Technology and Data Plan for information on how to access the backups of Job Responsibilities and Tasks Guide (Appendix D), if needed.
- If data needed to support ballot creation is lost or access to the data is unavailable, retrieve the backups of the needed data. This data includes:
  - Ballot design templates
  - The final version of approved candidate and proposition information to be included on ballot
  - Instructions on programming voting machines with ballot information
  - Documented ballot creation and voting machine programming job functions
- Two copies of the encrypted external hard drives with data backups are regularly updated once per month and stored offline. One is stored [onsite on the third floor and at road & bridge in our election room].
- When using the backed-up data, continue to follow data management policies according to the Election Data Classification System in the Election Information Security Policy.
- During elections, the final ballots must be stored electronically offsite in a location that only the Election Coordinator can quickly access and send to print should voting machines become inoperable and paper ballots become necessary. Refer to the Election Continuity of Operations Contact List (Appendix A) for the contact information of the printer standing by for immediate response if this situation arises.
- During elections, the Election Systems & Software is on call to assist with ballot issues or recovery processes. Refer to the Responsibility Succession Plan (Appendix C) and Election Continuity of Operations Contact List (Appendix A).

- The Loretta Mason must contact the insurance company that holds the cyber incident and disaster insurance policy to arrange coverage for the cost of replacing voting machines lost to damaging events, if applicable. Refer to the Election Continuity of Operations Contact List (Appendix A) for contact information.

Table 4: Ballot Creation and Distribution Alternative Technology and Data Plan

WHAT IS COMPROMISED	ALTERNATIVE	LOCATION	HOW TO ACCESS IT	ROLE WITH ACCESS OR RESPONSIBILITY TO TAKE ACTION			
				PRIMARY	DESK PHONE	NEXT-IN-LINE	DESK PHONE
ES&S creates our ballots	I would have to contact ES&S Ariela Matravers 469-675-8954	N/A	N/A	Election Coordinator	903-754-7275	Deputy EA/VR	123-456-7890
Access to Candidate Information	Candidate Data Backup is in binders on the 3 <sup>rd</sup> floor	Locked 3 <sup>rd</sup> floor election room	Loretta & Kelsey have keys to this room	Election Coordinator	903-754-7275	Deputy EA/VR	903-754-7924



# PLAN

Access to Master Ballot Design Template Electronic File	Located with ES&S	N/A	N/A	Election Coordinator	903-754-7275	Deputy EA/VR	903-754-7924
Primary Staff Member(s) Responsible for Creating Ballots	Next-in-Line Designee Follows Documented Job Duties	Documents in Election WISP binder in locked 3 <sup>rd</sup> floor election room	Loretta & Kelsey have keys to this room	Election Coordinator	903-754-7275	Deputy EA/VR	903-754-7275

## ePOLLBOOK AND VOTER CHECK-IN AND QUALIFICATION

This section references the underlying technologies and processes that enable the County Election Department to generate and distribute ePollbooks and facilitate the voter check-in process.

- The Loretta Mason is responsible for overseeing ePollbook programming or the creation of the paper Official List of Registered Voters (OLRV) with support from the Loretta Mason and election system vendors.
  - These systems and resources may include:
    - ePollbooks
    - Access to voter registration system
    - Internet access through a Virtual Private Network (VPN)
  - Refer to Table 5: ePollbook/Voter Check-In and Qualification Alternate Technology and Data Plan for information about technology and data sources that should be used if any of these resources is compromised.
- Refer to the Responsibility Succession Plan (Appendix C) to find who should be contacted if the Loretta Mason is not available.
  - The Elections Administrator, Loretta Mason is responsible for ensuring that the next-in-line designee has the required login credentials and the appropriate level of access permissions needed if the next-in-line designee must take over the role. The Elections Administrator, Loretta Mason should also ensure that the next-in-line designee understands ePollbook programming or the creation of the paper Official List of Registered Voters (OLRV) process.
- Next-in-line designees must refer to the Job Responsibilities and Tasks Guide (Appendix D) and follow the instructions for assuming the responsibilities of the role.
  - These documents are stored with the Election Written Information Security Program (WISP) in an electronic format backed up to two encrypted external hard drives, one stored securely onsite on the 3<sup>rd</sup> floor election room and one

stored offsite at Road & Bridge election room]. The documents will also be maintained in a paper format in the Election WISP binder stored & locked in the 3<sup>rd</sup> floor election room.

- Refer to Table 5: ePollbook/Voter Check-In Alternative Technology and Data Plan for information on how to access the backups of job process documentation, if needed.
- If data needed to support ePollbook creation is lost, or if access to the data is unavailable, retrieve the backups of the needed data. This data includes:
  - Voter registration data
  - ePollbook and paper OLRV design templates
  - Instructions on programming ePollbooks with voter check-in/qualification information
  - Documented ePollbook and voter check-in/qualification job functions
- Two copies of the encrypted external hard drives with data backups are regularly updated once per month or daily during the voting period and stored offline. One is stored onsite on the 3<sup>rd</sup> floor election room & road & bridge election room.
- When using the backed-up data, continue to follow data management policies according to the Election Data Classification System in the Election Information Security Policy.
- **Paper OLRV Counties** – During elections, the final Official List of Registered Voters (OLRV) should be stored in an electronic file both in house and offsite in the event that voter qualification must take place over the phone.
- **ePollbook Counties** – During elections, the final voter registration ePollbook electronic file and a printed copy of the paper OLRV are stored both in house and at an offsite location so that the Elections Administrator can quickly access and send to print should ePollbooks become inoperable and backup paper OLRVs become necessary. Contact the pre-designated printing company

capable of rapid bulk printing that is standing by for immediate response if this situation arises. Refer to the Election Continuity of Operations Contact List (Appendix A) for contact information of the printing company.

- During elections, ES&S] is on call to assist with ballot issues or recovery processes. Refer to the Responsibility Succession Plan (Appendix C) and Election Continuity of Operations Contact List (Appendix A).
- The Elections Administrator must contact the Auditor’s office to contact the insurance company that holds the cyber incident and disaster insurance policy to arrange coverage for the cost of replacing ePollbooks lost to damaging events, if applicable. Refer to the Election Continuity of Operations Contact List (Appendix A) for contact information.

Table 5: ePollbook/Voter Check-In and Qualification Alternative Technology and Data Plan

WHAT IS COMPROMISED	ALTERNATIVE	LOCATION	HOW TO ACCESS IT	ROLE WITH ACCESS OR RESPONSIBILITY TO TAKE ACTION			
				PRIMARY	DESK PHONE	NEXT-IN-LINE	DESK PHONE
Internet Access to Voter Registration System	Mobile Hotspot Device 1	Locked 3 <sup>rd</sup> floor election room	Loretta & Kelsey have keys to this room	Voter Registrar	903 754-7275	Deputy EA/VR	903-754-7924

# PLAN

One ePollbook	Spare ePollbook 2	1 <sup>st</sup> floor election room	N/A	Voter Registrar	903-754-7275	Deputy EA/VR	903-754-7924
All ePollbooks	Contact Equipment Vendor to Initiate Previously Negotiated Emergency Equipment Replacement Plan	N/A	Contact Info: Rep Name Phone 972- 533-5559 Email: <a href="mailto:chris.moody@essvote.com">chris.moody@essvote.com</a>	Voter Registrar	903-754-7275	Deputy EA/VR	903-754-7924
All ePollbooks	Flash drive from ES&S for ePollbooks	3 <sup>rd</sup> floor election room	Loretta & Kelsey have keys to it	Voter Registrar	903-754-7275	Deputy EA/VR	903-754-7924
Primary Staff Member(s) Responsible for ePollbook	Next-in-Line Designee Follows	Documents in Election WISP binder in locked 2 <sup>nd</sup>	Loretta & Kelsey have keys to it	Voter Registrar	903-754-7275	Deputy EA/VR	903-754-7924

Creation and Voter Check-In	Documented job Duties	floor storage closet, or on backup hard drive					
--------------------------------	--------------------------	--	--	--	--	--	--



## VOTE CASTING AND CAPTURE

This section references the underlying technologies and processes that enable the County Election Department to facilitate vote casting and capture.

- The Elections Administrator is responsible for regularly testing voting machines' functionality to ensure that they are operating correctly and for arranging transport to and from polling locations with support from the ES&S election system vendors.
  - These systems and resources include:
    - Voting machines
      - Acceptance testing
      - Preparation prior to election
      - Hardware testing
      - Logic and accuracy testing
      - Post-election maintenance
  - Refer to Table 6: Vote Casting and Capture Alternative Technology and Data Plan for information about technology and data sources that should be used if any of these resources is compromised.
- Refer to the Responsibility Succession Plan (Appendix C) to find who must be contacted if the Election Administrator is not available.
  - The Election Administrator is responsible for ensuring that the next-in-line designee has the required login credentials and the appropriate level of access permissions needed if the next-in-line designee must take over the role. The Election

Administrator should also ensure that the next-in-line designee understands the vote casting and capture process and knows how to troubleshoot common voting machine issues.

- Next-in-line designees must refer to the Job Responsibilities and Tasks Guide (Appendix D) and follow the instructions for assuming the responsibilities of the role.
  - These documents are stored with the Election Written Information Security Program (WISP) in an electronic format backed up to two encrypted external hard drives, one stored securely onsite in the on the 3<sup>rd</sup> floor election room and one stored offsite at Road & Bridge election room. The documents will also be maintained in a paper format in the Election WISP binder stored in the 3<sup>rd</sup> floor election room.
  - Refer to Table 6: Vote Casting and Capture Alternative Technology and Data Plan for information on how to access the backups of Job Responsibilities and Tasks Guide, if needed.
  - If data needed to support vote casting and capture is lost, or if access to the data is unavailable, retrieve the backups of the needed data. This data includes:
    - Inventory of voting machines
    - Instructions on testing voting machines
    - Instructions on operating voting machines
    - Documented voting machine operations and maintenance job functions
  - Retrieval of data may involve returning equipment to the manufacturer or vendor
    - Acceptance testing after equipment is repaired by vendor
  - Two copies of the encrypted external hard drives with data backups are regularly updated once per month and stored offline. One is stored in the 3<sup>rd</sup> floor election room and at Road & Bridge election room.

- When using the backed-up data, continue to follow data management policies according to the Election Data Classification System in the Election Information Security Policy.
- During elections, the ES&S is on call to assist with voting machine issues or recovery processes. Refer to the Responsibility Succession Plan (Appendix C) and Election Continuity of Operations Contact List (Appendix A).
- The Election Administrator must contact the Auditor to contact the insurance company that holds the cyber incident and disaster insurance policy to arrange coverage for the cost of replacing voting machines lost to damaging events, if applicable. Refer to the Election Continuity of Operations Contact List (Appendix A) for contact information.

Table 6: Vote Casting and Capture Alternative Technology and Data Plan

WHAT IS COMPROMISED	ALTERNATIVE	LOCATION	HOW TO ACCESS IT	ROLE WITH ACCESS OR RESPONSIBILITY TO TAKE ACTION			
				PRIMARY	DESK PHONE	NEXT-IN-LINE	DESK PHONE

<p>Many or All Voting Machines</p>	<p>Contact ES&amp;S to get replacement equipment or have a member come work on equipment</p>	<p>N/A</p>	<p>Chris Moody 972-533- 5559 Phone # Email</p>	<p>Loretta Mason</p>	<p>903-754-7275</p>	<p>Kelsey Gates</p>	<p>903-754-7924</p>
--	--	------------	--	--------------------------	---------------------	---------------------	---------------------

# PLAN

Primary Staff Member(s) Responsible for Testing and Managing Voting Machines	Next-in-Line Designee Follows Documented Job Duties	Documents in Election WISP binder in Locked 3 <sup>rd</sup> floor election room or on back up drive located at Road & Bridge Election room	Loretta or Kelsey has a key to this room	Loretta Mason	903-754-7275	Kelsey Gates	903-754-7924
--	---	--	--	---------------	--------------	--------------	--------------

## VOTE TABULATION

This section references the underlying technologies and processes that enable the County Election Department to count votes and determine results.

- The Central Counting Station Manager, Loretta Mason is responsible for testing the tabulation computer prior to the election and collecting and tabulating votes into final counts in a secure manner with the required two-person validation support from Kelsey Gates, Tabulation Supervisor.
  - The required include:
    - Tabulation computer
    - Testing materials
  - Refer to Table 7: Vote Tabulation Alternative Technology and Data Plan for information on technology and data sources that should be used if any of these resources is compromised.
- Refer to the Responsibility Succession Plan (Appendix C) to find who should be contacted if the Elections Administrator is not available.
  - The Central Counting Station Manager is responsible for ensuring that the next-in-line designees have the required login credentials and the appropriate level of access permissions needed if the next-in-line designees must take over the tabulation roles. The Central Counting Station Manager should also ensure that the next-in-line designees understand how to test the tabulation computer before an election as well as the process of tabulating votes and the importance of two-person validation. Individuals selected for this job must be able to accurately perform the duties at the end of a long day.



- Next-in-line designees must refer to the Job Responsibilities and Tasks Guide (Appendix D) and follow the instructions for assuming the responsibilities of the role.
  - These documents are stored with the Election Written Information Security Program (WISP) in an electronic format backed up to two encrypted external hard drives, one stored securely onsite in the 3<sup>rd</sup> floor election room and one stored offsite at Road & Bridge Election room. The documents will also be maintained in a paper format in the Election WISP binder stored in the 3<sup>rd</sup> floor election room.
  - Refer to Table 7: Vote Tabulation Alternative Technology and Data Plan for information on how to access the backups of the Job Responsibilities and Tasks Guide (Appendix D), if needed.
  - If data needed to support vote tabulation is lost, or if access to the data is unavailable, retrieve the backups of the needed data. This data includes:
    - Instructions on testing the tabulation computer
    - Instructions on operating the tabulation computer
    - Instructions on repairing or replacing the tabulation computer
    - Procedures for replacing the tabulation computer in the middle of an election
    - Documented vote tabulation job functions
  - Two copies of the encrypted external hard drives with data backups are regularly updated once per month and stored offline. One is stored 3<sup>rd</sup> floor election room and the other offsite Road & Bridge election room.
  - When using the backed-up data, continue to follow data management policies according to the Election Data Classification System in the Election Information Security Policy.

- An arrangement for repairing or replacing the tabulation computer in the middle of an election has been made with the vendor. During elections, the procedures and instructions for repairing or replacing the tabulation computer are printed and posted near the tabulation computer with the contact number for the vendor. *ES&S\_vendor* is on call to assist with recovery processes during elections. Refer to the Election Continuity of Operations Contact List (Appendix A) for contact information.
- Vote tabulation should take place in a pre-designated secured counting room. If the counting room is not usable, or if power is not available, Expo Hall will be the alternate counting room. Refer to the Alternate Utilities and Facilities Plan (Appendix E) for details on when and how to relocate if necessary.
- If relocation is needed, refer to the Relocation Checklist (Appendix F) to make sure all needed items are transported and set up at the alternate site.
- The Election Administrator the county auditor and in turn they will contact the insurance company that holds the cyber incident and disaster insurance policy to arrange coverage for the cost of replacing tabulation computers lost to damaging events, if applicable. Refer to the Election Continuity of Operations Contact List (Appendix A) for contact information.

Table 7: Vote Tabulation Alternative Technology and Data Plan

WHAT IS COMPROMISED	ALTERNATIVE	LOCATION	HOW TO ACCESS IT	ROLE WITH ACCESS OR RESPONSIBILITY TO TAKE ACTION			
				PRIMARY	DESK PHONE	NEXT-IN-LINE	DESK PHONE

# PLAN

ERM	Do not have a backup tabulation computer	Locked in the 3 <sup>rd</sup> floor election room	Loretta Mason & Kelsey Gates have keys to this room	Central Counting Station Manager Loretta Mason	903-754-7275	Tabulation Supervisor Kelsey Gates	903-754-7924
Backup Tabulation Computer, ES&S would have to overnight	Contact Equipment Vendor to Initiate Previously Negotiated Emergency Equipment Replacement Plan	N/A	Chris Moody 972-533-5559 Chris.moody@essvote.com	Central Counting Station Manager Loretta Mason	903-754-7275	Tabulation Supervisor  Kelsey Gates	903-754-7924
Primary Staff Member(s) Responsible for Testing & Tabulation	Next-in-Line Designee Follows Documented Job Duties	Documents in Election WISP binder in locked 3 <sup>rd</sup> floor	Key to closet, 3 <sup>rd</sup> floor election room & Road &	Central Counting Station Manager	903-754-7275	Tabulation Supervisor	903-754-7924

<p>Computer and Tabulating Votes Loretta Mason</p>	<p>Kelsey Gates</p>	<p>election room</p>	<p>Bridge Election room Loretta Mason &amp; Kelsey Gates are the only ones who have these keys</p>	<p>Loretta Mason</p>		<p>Kelsey Gates</p>	
--	---------------------	--------------------------	--	----------------------	--	---------------------	--

## ELECTION NIGHT REPORTING

This section references the underlying technologies and processes that enable the County Election Department to securely report accurate results.

- The Election Administrator Loretta Mason is responsible for testing the election night reporting procedures prior to every election and for reporting the official election results.
  - The required systems include:
    - Secure computer
    - Internet connectivity to access the Secretary of State’s Election Night Reporting Interface
    - Device, cell phone, or application needed for multi-factor authentication
    - Batteries and chargers to keep computer, phone, and devices charged
    - County election website
  - Refer to Table 8: Election Night Reporting Alternative Technology and Data Plan for information on technology and data sources that should be used if any of these resources is compromised.
- Refer to the Responsibility Succession Plan (Appendix C) to find who should be contacted if the Election Administrator, Loretta Mason is not available.
  - The Election Administrator, Loretta Mason is responsible for ensuring that the next-in-line designee has the required login credentials and the appropriate level of access permissions needed if the next-in-line designee must take over the role. The Election Administrator, Loretta Mason should also ensure that the next-in-line designee understands the election night reporting process and the sensitivities involved.

- Next-in-line designees must refer to the Job Responsibilities and Tasks Guide (Appendix D) and follow the instructions for assuming the responsibilities of the role.
    - These documents are stored with the Election Written Information Security Program (WISP) in an electronic format backed up to two encrypted external hard drives, one stored securely onsite in the 3<sup>rd</sup> floor election room, and one stored offsite at Road & Bridge . The documents will also be maintained in a paper format in the Election WISP binder stored in the 3<sup>rd</sup> floor election room.
    - Refer to Table 8: Election Night Reporting Alternative Technology and Data Plan for information on how to access the backups of the Job Responsibilities and Tasks Guide (Appendix D), if needed.
    - If data needed to support election night reporting is lost, or if access to the data is unavailable, retrieve the backups of the needed data. This data includes:
      - Instructions on accessing the Secretary of State’s election night reporting interface including the two-step multi-factor authentication login
      - Instructions on posting results to the county’s official website and using social media only to direct the public to the county’s official website for results
      - Documented election night reporting and publishing job functions
    - Two copies of the encrypted external hard drives with data backups are regularly updated once per month and stored offline. One is stored in the 3<sup>rd</sup> floor election room and the other offsite at the Road & Bridge election room.
- When using the backed-up data, continue to follow data management policies according to the Election Data Classification System in the Election Information Security Policy.

- Prior to the election, the Election Administrator Loretta Mason will have added the Secretary of State Hotline Number as a contact on their cell phone and programmed with speed dial. If the alternative technologies in Table 8: Election Night Reporting Alternative Technology and Data Plan fail, the Election Administrator, Loretta Mason will call in the election results to the Secretary of State’s hotline.
- Election night reporting is pre-designated to take place in the Election Administrator’s office, which ensures reliable internet access and access to the multi-factor authentication methods required to report to the Secretary of State. If the Election Administrator’s office is not usable, or if power is not available, the Expo Hall located on Ballpark drive, Carthage, Tx. Refer to the Alternate Utilities and Facilities Plan (Appendix E) for details on when and how to relocate if necessary.

If relocation is needed, refer to the Relocation Checklist (Appendix F) to make sure all needed items are transported and set up at the alternate site.

Table 8: Election Night Reporting Alternative Technology and Data Plan

WHAT IS COMPROMISED	ALTERNATIVE	LOCATION	HOW TO ACCESS IT	ROLE WITH ACCESS OR RESPONSIBILITY TO TAKE ACTION			
				PRIMARY	DESK PHONE	NEXT-IN-LINE	DESK PHONE



# PLAN

Computer Needed to Report Result	Prepared replacement computer 1 Elections Administrators computer	Loretta's desk	N/A	Election Administrator  Loretta Mason	903-754-7275	Deputy EA/VR  Kelsey Gates	903-754-7924
Computer Needed to Report Results	Prepared replacement computer 2 Deputy EA/VR computer	Kelsey's desk	N/A	Election Administrator  Loretta Mason	903-754-7275	Deputy EA/VR  Kelsey Gates	903-754-7924
Internet Access to SOS and County Election Website	Mobile Hotspot Device 1	Locked 3 <sup>rd</sup> floor election room	Loretta & Kelsey have keys to this room	Election Administrator	903-754-7275	Deputy EA/VR	903-754-7924

NAME	TITLE	PHONE	ALTERNATE/ CELL PHONE	EMAIL	STREET ADDRESS	DEPARTMENT/ VENDOR/ AGENCY
Loretta Mason	Election Administrator	903-693-0370	903-754-7275	<a href="mailto:lmason@co.panola.tx.us">lmason@co.panola.tx.us</a>	110 S Sycamore St., Room 100, Carthage, Tx. 75633	County Election Department
Chris Moody	Sales	972-533-5559		<a href="mailto:chris.moody@essvote.com">chris.moody@essvote.com</a>	1217 Digital Drive, Suite 160, Richardson, Tx 75081	ES&S Sales
Cutter Clinton	Sheriff	903-693-0333		<a href="mailto:cutter.clinton@co.panola.tx.us">cutter.clinton@co.panola.tx.us</a>	314 W. Wellington St., Carthage, Tx 75633	Sheriff's Department
Bryan Murff	Emergency Management Coordinator	903-754-1433		<a href="mailto:bryan.murff@co.panola.tx.us">bryan.murff@co.panola.tx.us</a>	110 S. Sycamore St. Carthage, Tx 75633	Emergency Response Coordinator
Rodger McLane	County Judge	903-693-0391		<a href="mailto:rodger.mclane@co.panola.tx.us">rodger.mclane@co.panola.tx.us</a>	110 S. Sycamore St., Carthage, Tx 75633	

Barry Tate	IT Admin	903-261-7864		itadmin@co.panola.tx.us		110 S Sycamore St., Carthage, Tx 75633
------------	----------	--------------	--	-------------------------	--	--

APPENDIX A: ELECTION CONTINUITY OF OPERATIONS CONTACT LIST

This list must be maintained and updated regularly once per month with contact information for all staff members, agencies, and entities involved in ensuring the continuity of operations during a cyberattack or disaster event. This list is not the same as the Incident Response List in the Security Incident Response Plan although some contacts may be on both lists. This list is for distribution to a wider group of staff members with responsibilities for keeping operations running during an attack or disaster.

An electronic copy of the contact list must be available to staff and included in the data backup every month. Additionally, a paper copy must be kept in a file in the Election Administrator’s office. **Managers and employees with Incident Response and Continuity of Operations duties must keep these names and numbers programmed into their phone contact lists for quick reference.**

APPENDIX B: EARLY VOTING AND ELECTION DAY WORKER CONTACT LIST

In addition to the Election Continuity of Operations Contact List (Appendix A) maintained year-round, an Early Voting and Election Day Worker Contact List (Appendix B) must be maintained and updated regularly weekly during the two months preceding an election with contact information for all early voting and election day workers and personnel that interact with and manage early voting and election day workers through the course of managing and facilitating elections.

- During elections, designate an early voting and election day worker coordinator as a single point of contact for communicating emergency and/or alternative procedure instructions and for receiving information from early voting and election day workers in the event of a cyberattack or disaster event.

A copy of the list must be retained and included in the data backup monthly during the two months preceding the election.

Additionally, a paper copy will be maintained in the election emergency preparedness binder.

NAME	EARLY VOTING AND ELECTION DAY WORKER TITLE	PHONE	ALTERNATE/CELL PHONE	EMAIL	LOCATION
Marian Foster	EVBB member	903-693-8607			3 <sup>rd</sup> floor election room
Wanda Gaines	EVBB member	903-806-3243			3 <sup>rd</sup> floor election room
Lynn Getsay	EVBB member	903-472-3868			3 <sup>rd</sup> floor election room
Petrice Roberson	EVBB member	318-426-4492			3 <sup>rd</sup> floor election room
Gail Hudman	EVBB member	281-610-4300			3 <sup>rd</sup> floor election room

# PLAN

Kirby Hill	ED	903-261-5224			Box 1
Peggy Hill	ED	903-261-5224			Box 1
Gary Henderson	ED	903-692-0320			Box 1
Lindsey Coleman	ED	903-263-4919			Box 2
Margaret Thompson	ED	903-272-1306			Box 2
Hazel Sorters	ED	903-930-6846			Box 3
Kandace Fortune	ED	281-460-6041			Box 3
Paulette Goree	ED	903-424-8648			Box 3
Elizabeth Ross	ED	903-930-6846			Box 3
Gloria Adams	ED	903-692-6807			Box 3
Cecilia English	ED	903-754-9696			Box 5
Gene Williams	ED	903-746-7062			Box 5
Keith Williams	ED	903-646-2149			Box 5
Tammy Light	ED	903-263-5145			Box 7
Mary Jo Anderson	ED	903-766-3860 310-867-1381			Box 7
Carolyn Powell	ED	903-263-5145			Box 7
Taunya Vance	ED	903-754-8192			Box 8
Brandi Pierce	ED	903-472-2429			Box 8
Mike Vance	ED	903-930-2182			Box 8
Barbara Burns	ED	903-263-8694			Box 9
Nancy Oden	ED	903-690-1302			Box 9

# PLAN

Bridgitte Hickey	ED	903-263-9688			Box 10
Patricia Aaron	ED	903-263-1471			Box 10
Liz Harrison	ED	903-754-7683			Box 12
Karen Marsalis	ED	985-630-6853			Box 12
Patricia Robinson	ED	318-465-8277			Box 12
Patricia Dock	ED	903-263-4620			Box 12
Vera Knight	ED	936-248-5764			Box 13
Jessica Mosley	ED				Box 13
Oscar Mosley	ED	903-280-1538			Box 13
Ronnie Nutt	ED	903-754-0996			Box 14
Katherine White	ED	903-685-2574			Box 14
Travis Nutt	ED	903-754-0995			Box 14
Lycia Evanoff	ED	903-261-9006			Box 18
Michael Sikorski	ED	307-231-5461			Box 18
Barbara Cordell	ED	936-554-7678			Box 18
Joe Bartnik	ED	936-556-2728			Box 18
Wayne Wimberly	ED	936-591-1005			Box 19
Leona Wimberly	ED	903-930-5554			Box 19

# PLAN

Hunter Marceaux	ED	903-690-3679			Box 20
Kathy Porter	ED	903-754-0965			Box 22
Danyel Clements	ED	903-263-2377			Box 22
Gloria Brooks	ED	903-806-3251			Box 22
Lawanda Williams	ED	903-241-5408			Box 22
Dan Harrison	ED	903-631-0241			Box 27
James Brown	ED	430-258-9614			Box 27
James Marshall	ED	903-387-7068			Box 27
Chantal Hedlund	ED	936-427-7215			Box 28
Kim Bacon	ED	214-288-8265			Box 28
Sharleen Pelzl	ED	512-827-6573			Box 28
Shirley Buchanan	ED	512-999-1454			Box 28
Jennifer Journeycake	ED	903-263-8079			Box 29
Connie May	ED	903-263-4817			Box 29
Lori Cordova	ED	903-754-7436			Box 29
Ken Walker	ED	903-472-9781			Box 29



APPENDIX C: RESPONSIBILITY SUCCESSION PLAN

If a team member or critical vendor contact is unable to perform the assigned role, that person’s duties must become the responsibility of an assigned individual specified in the following table. It is the responsibility of each primary individual to document the functions of the job, including how to access locked and secured assets and to train the next-in-line designee on what will be required to take over the role. Additionally, access credentials and administrative permissions must be established for the next-in-line individual.

ROLE	DUTIES	PRIMARY	MOBILE #	NEXT-IN-LINE DESIGNEE	MOBILE #	NEXT-IN-LINE HAS DOCUMENTED JOB FUNCTIONS?	NEXT-IN-LINE HAS NEEDED CREDENTIALS AND PERMISSIONS?
Election Administrator	<ul style="list-style-type: none"> <li>Maintain Election Operations During Incident</li> <li>Determine the Appropriate Continuity Plan Elements to Enact</li> <li>Determine the Needed Replacement/Backup Equipment, Technology and Supplies to Deploy</li> <li>Immediately Restore Critical Data from</li> </ul>	Loretta Mason	903-754-7275	Kelsey Gates	903-754-7924	Yes	Yes

	<ul style="list-style-type: none"> <li>Backup Hard Drive if Needed</li> <li>Notify Secretary of State's Office</li> <li>Follow Incident Response Plan Procedures if Incident Is Severe Enough</li> <li>Notify Law Enforcement, State DIR and Any Other Entities Necessary</li> </ul>						
Voter Registrar	<ul style="list-style-type: none"> <li>Maintain Access to Voter Registration Data</li> <li>Protect Data from Compromise</li> <li>Create Ballots</li> <li>Program Ballots into Voting Machines</li> </ul>	Loretta Mason	903-754-7275	Kelsey Gates	903-154-7924	Yes	Yes
IT Director	<ul style="list-style-type: none"> <li>Determine Severity of the Incident</li> <li>Restore Full Operability as Quickly as Possible</li> <li>Advise Affected Staff on How to Stop Further Damage</li> <li>Advise Staff on Which Systems Are Operational and Which Are Unavailable During Mitigation</li> </ul>	Barry Tate	903-261-7864	Does not have a backup		No	No

# PLAN

	<ul style="list-style-type: none"> <li>• Mitigate Cyber Incident</li> <li>• Assemble the Technical IR Team Members</li> </ul>						
Early Voting and Election Day Worker Coordinator	<ul style="list-style-type: none"> <li>• Inform Early Voting and Election Day Workers of Emergency or Temporary Operations and Procedures</li> <li>• Notify EA of Issues at Polling Locations</li> </ul>	Loretta Mason	903-754-7275	Kelsey Gates	903-754-7924	Yes	No
Office Manager	<ul style="list-style-type: none"> <li>• Maintain Operations</li> <li>• Program Data into ePollbooks</li> <li>• Assemble the Needed Backup Technology, Equipment, Information and Supplies</li> </ul>	Loretta Mason	903-754-7275	Kelsey Gates	903-754-7924	Yes	Yes
Communications Director	<ul style="list-style-type: none"> <li>• Inform the Media According to the Data Classification System</li> <li>• Serve as Point of Contact for All Information Flowing in and Out of Election Department</li> <li>• Keep EA Informed of Developments and</li> </ul>	Loretta Mason	903-754-7275	Kelsey Gates	903-754-7924	Yes	Yes

# PLAN

	<ul style="list-style-type: none"> <li>Communication Activities</li> <li>Facilitate Communication Between Departments Involved</li> </ul>						
Voting System Vendor	<ul style="list-style-type: none"> <li>Maintain Voting System Operability</li> </ul>	Loretta Mason	903-754-7275	Kelsey Gates	903-754-7924	Yes	Yes
ePollbook Vendor	<ul style="list-style-type: none"> <li>Maintain ePollbook Operability</li> </ul>	Loretta Mason	903-754-7275	Kelsey Gates	903-754-7924	Yes	Yes
Cyber Incident and Election Equipment Insurance Provider, if applicable	<ul style="list-style-type: none"> <li>Cover Cost of Damage Caused by Cyber Incident and Election Equipment Replacement</li> </ul>	TAC Jennifer Stacy (Auditor)	903-693-0321	Todd Kissel	800-456-5974	N/A	N/A

APPENDIX D: JOB RESPONSIBILITIES AND TASKS GUIDE

All personnel responsible for essential business functions must make a copy of this table and use it to document their job processes in a detailed, step-by-step format that is easy for a next-in-line designee to follow if the responsible person is unavailable to perform the duties and the next-in-line designee must assume the role.

JOB RESPONSIBILITIES AND TASKS GUIDE			
Title: Election Coordinator			
Critical Responsibilities	Step-by-Step Task Instructions	Resources Needed	Resource Location
Step by step check list for elections	Following each item on list	<ul style="list-style-type: none"> <li>Check list</li> </ul>	EA's desktop

APPENDIX E: ALTERNATE UTILITIES AND FACILITIES PLAN

If a building is rendered unusable due to a power failure or disaster event, the following table describes the planned steps for a temporary solution or where to relocate to in order to keep operations running.

ISSUE	SOLUTION	CONTACT	ESTIMATED COSTS	WHO IS RESPONSIBLE FOR TAKING ACTION			
				PRIMARY	MOBILE #	NEXT-IN-LINE DESIGNEE	MOBILE #
Short Term Electricity	Our Fire departments	Bryan Murff 903-754-1433	\$0.00	Loretta Mason	903-754-754-7275	Kelsey Gates	903-754-7924

# PLAN

Outage at Election Main Office	have backup generators that we have permission to use						
Longer Duration Electricity Outage at Election Main Office	Set up temporarily at Expo Hall located on ballpark drive Carthage, Tx 75633 Per our County Judge.	Tommy Earle 903-692-2844	\$.00	Loretta Mason	903-754-7275	Kelsey Gates	903-754-7924
Electricity Outage at Polling Location	Our Fire departments have backup generators that we have permission to use	Bryan Murff 903-754-1433	\$ 00	Loretta Mason	903-754-7275	Kelsey Gates	903-754-7924
Election Main Office Is Unusable	Set up Temporarily at the Expos Hall	Tommy Earle 903-692-2844	\$.00	Loretta Mason	903-754-7275	Kelsey Gates	903-754-7924

# PLAN

	located on Ballpark Drive, Carthage, Tx 75633 per the County Judge.						
Counting Room and Election Main Office is Unusable for Tabulation	Set up Temporarily at the Expo Hall located on Ballpark Drive, Carthage, Tx 75633l.	Tommy Earle 903-692-2844	\$ .00	Loretta Mason	903-754- 7275	Kelsey Gates	903-754- 7924
Box 1	Chapel at Panola College	Mary Chance 903-693-1142	\$ .00	Loretta Mason	903-754- 7275	Kelsey Gates	903-754- 7924
Box 2	St. Johns Church	Rev. Jennene 903-235-6825	\$100.00	Loretta Mason	903-754- 7275	Kelsey Gates	903-754- 7924
Box 3	Mt. Zion Baptist Church	Keith Williams 903-646-2149	\$ .00	Loretta Mason	903-754- 7275	Kelsey Gates	903-754- 7924
Box 5	Beckville Community Center	City of Beckville	\$100 00	Loretta Mason	903-754- 7275	Kelsey Gates	903-754- 7924



# PLAN

Box 7	Community 4 Fire Station	Barbara Burns	\$100.00	Loretta Mason	903-754- 7275	Kelsey Gates	903-754- 7924
Box 8	Inter Community Fire Station 134 FM 1186 DeBerry, Tx 75639	Bryan Murff 903-754-1433	\$ 00	Loretta Mason	903-754- 7275	Kelsey Gates	903-754- 7924
Box 9	Community 4 VFD Sub Station	Barbara Burns	\$100.00	Loretta Mason	903-754- 7275	Kelsey Gates	903-754- 7924
Box 10	Inter Community Fire Station 134 FM 1186 DeBerry, Tx 75639	Bryan Murff 903-754-1433	\$100.00	Loretta Mason	903-754- 7275	Kelsey Gates	903-754- 7924
Box 12	Move to gym and or fire station	Bryan Murff 903-754-1433	\$100.00	Loretta Mason	903-754- 7275	Kelsey Gates	903-754- 7924
Box 13	Old Center Community Center	Wayne Wimberly	\$100.00	Loretta Mason	903-754- 7275	Kelsey Gates	903-754- 7924
Box 14	Gary Store	Mrs. Jerrie	\$0.00	Loretta Mason	903-754- 7275	Kelsey Gates	903-754- 7924

# PLAN

Box 18	Clayton Fire Department	Bryan Murff 903-754-1433	\$100.00	Loretta Mason	903-754-7275	Kelsey Gates	903-754-7924
Box 19	Woods Fire Department	Bryan Murff 903-754-1433	\$100 00	Loretta Mason	903-754-7275	Kelsey Gates	903-754-7924
Box 20	Gary Fire Department 4712 FM 10 Gary, Tx 75643	Mark Dawson 903-754-1835	\$100.00	Loretta Mason	903-754-7275	Kelsey Gates	903-754-7924
Box 22	Inter Community Fire Station 134 FM 1186 DeBerry, Tx 75639	Bryan Murff 903-754-1433	\$100.00	Loretta Mason	903-754-7275	Kelsey Gates	903-754-7924
Box 26	Dead Wood Community Center	Butch Marsalis 985-807-4401	\$100 00	Loretta Mason	903-754-7275	Kelsey Gates	903-754-7924
Box 27	Bethlehem Baptist Church	Rev. J.T. Harris 903-690-2310	\$100 00	Loretta Mason	903-754-7275	Kelsey Gates	903-754-7924
Box 28	Expo Hall Ball Park Drive	Tommy Earle 903-692-2844	\$.00	Loretta Mason	903-754-7275	Kelsey Gates	903-754-7924

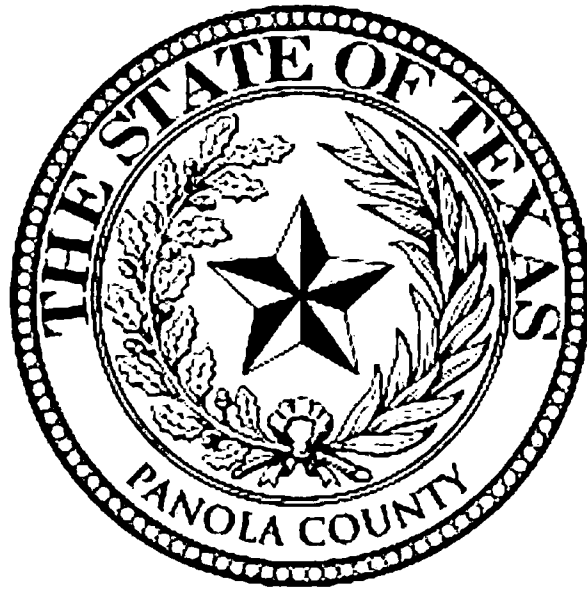
	Carthage, Tx 75633						
Box 29	Deadwood Community Center	Butch Marsalis 985-807-4401	\$100.00	Loretta Mason	903-754- 7275	Kelsey Gates	903-754- 7924

APPENDIX F: RELOCATION CHECKLIST

ITEM	LOCATION	WHO IS RESPONSIBLE
Computers	Individual Desks	Each Staff Member Is Responsible for His or Her Computer
Written Information Security Program Binder	Locked 3 <sup>rd</sup> floor election room	Election Administrator/Deputy EA/VR
Backup Hard Drive	Locked 3 <sup>rd</sup> floor election room	Election Administrator/Deputy EA/VR
Mobile Hotspot Device	Locked 3 <sup>rd</sup> floor election room	Election Administrator/Deputy EA/VR
Ds200, Express Votes, Ballot Boxes & EPollbooks	Locked 3 <sup>rd</sup> floor election room	Election Administrator/Deputy EA/VR
Main Tabulation Computer	Locked 3 <sup>rd</sup> floor election room	Election Administrator/Deputy EA/VR
Batteries and Chargers	Election Office	Election Administrator/Deputy EA/VR

Extension Cords	3 <sup>rd</sup> floor election room	Election Administrator/Deputy EA/VR
Seals, Locks, Keys	1 <sup>st</sup> floor election office	Election Administrator/Deputy EA/VR
Ballots, papers for election	Election office	Election Administrator/Deputy EA/VR

*PANOLA COUNTY  
ELECTIONS  
INCIDENT RESPONSE  
PLAN*





### **CONFIDENTIAL INFORMATION WARNING**

This document contains information about the security of Panola 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 Panola County Confidential, and cannot be reproduced, redistributed in any way, shape or form without prior written consent from Panola County.



## Contents

ELECTION INCIDENT RESPONSE PLAN.....	8
• STEP 1: DETERMINE IF THE EVENT IS A CONFIRMED SECURITY INCIDENT .....	8
• STEP 2: BEGIN DOCUMENTING THE RESPONSE .....	9
• STEP 3: NOTIFY LEADERSHIP STAKEHOLDERS .....	9
• STEP 4: NOTIFY AND ASSEMBLE THE INCIDENT RESPONSE TEAM .....	9
• STEP 5: ANALYZE THE EVENT FOR SCOPE AND START REPORT .....	10
TABLE 1: INCIDENT SEVERITY CLASSIFICATION SYSTEM .....	10
• STEP 6: SET UP A COMMAND CENTER .....	11
• STEP 7: ASSEMBLE INCIDENT RESPONSE RESOURCES .....	11
TABLE 2: INCIDENT RESPONSE RESOURCE LIST.....	11
• STEP 8: INITIATE THE CONTINUITY OF OPERATIONS PLAN .....	13
• STEP 9: WORK WITH THE IT STAFF TO CONTAIN THE DAMAGE .....	13
• STEP 10: NOTIFY THE INSURANCE PROVIDER, IF APPLICABLE.....	13
• STEP 11: INITIATE THE INTERNAL COMMUNICATIONS PLAN.....	14
• STEP 12: INITIATE THE EXTERNAL COMMUNICATIONS PLAN .....	15
• STEP 13: RECOVER THE ASSETS AND DATA .....	16
• STEP 14: DOCUMENT THE INCIDENT IN A CYBERSECURITY INCIDENT REPORT	16
• STEP 15: IDENTIFY LESSONS LEARNED AND UPDATE THE PLAN .....	16
• STEP 16: COLLECT AND SUBMIT EVIDENCE .....	17
APPENDIX A: INCIDENT HANDLER’S LOG AND REPORT .....	18
APPENDIX B: INCIDENT NOTIFICATION PRIORITY CONTACT LIST .....	20
APPENDIX C: INCIDENT RESPONSE TEAM ROLES AND RESPONSIBILITIES .....	22
APPENDIX D: EMERGENCY CONTACT LIST .....	26
APPENDIX E: COMMUNICATIONS PLAN.....	27
APPENDIX F: EVIDENCE / CHAIN OF CUSTODY FORM.....	29

# ELECTION INCIDENT RESPONSE PLAN

Panola County Elections must follow these steps to respond to a security incident:

## STEP 1: DETERMINE IF THE EVENT IS A CONFIRMED SECURITY INCIDENT

- Suspected cyber incidents must be immediately reported to the [Election Administrator or Designee] who is authorized to take the lead as the Incident Response Commander as defined in the Incident Response Team Roles and Responsibilities Chart (SEE APPENDIX C)
- The Incident Response Commander must submit the details of a possible cyber incident to [specify a role or entity that has the knowledge to decide if an attack has happened such as a staff member with cybersecurity training, IT staff member, IT or security vendor, or Texas Department of Information Resources (DIR)] to confirm validity before it is declared an incident. Potential attack methods should be considered when determining if an incident has occurred including:
  - Viruses from external/removable media
  - Email that triggered malware or ransomware
  - Email phishing campaigns that exposed access credentials resulting in a breach
  - Access to credential theft through hacking
  - Device, system or equipment tampering
  - Loss or theft of equipment
  - If there is doubt about the validity of a possible incident, escalate the issue to Barry Tate IT specialist to conduct a deeper analysis including, but not limited to looking for:
    - Changes in User IDs, Groups, Access Rights
    - File Modification Dates and Ownership
    - Network Configuration Changes and Unusual Activity
    - Unauthorized Applications Running
    - System Binaries
    - Altered Registry Keys
    - Unusual or Hidden Files
    - Modifications to Data or Configuration Files
    - Recent Changes, Failures, Errors, Status Changes, Access/admin Events
    - Access to credentials through hacking or social engineering

## STEP 2: BEGIN DOCUMENTING THE RESPONSE

- If the event is determined to be a security incident, the Incident Response Commander must immediately begin tracking response activities in an Incident Handler's Log and Report that will be submitted to the Texas Secretary of State's Office after the incident is remediated. (SEE APPENDIX A).
- Incident Handlers are the individuals on the Incident Response Team (see Notify and Assemble the Incident Response Team in Step 4) who coordinate and execute the efforts to contain the incident, minimize the damage, and begin recovery.
- The Incident Response Commander must record facts, theories and rumors in the Incident Handler's Log and Report to minimize the potential for making misguided decisions or communicating false information.

## STEP 3: NOTIFY LEADERSHIP STAKEHOLDERS

- The Election Administrator, Loretta Mason must notify all critical stakeholders (only inform those who need to know) at this phase of the response process. Refer to the contact information listed in the Incident Notification Priority Contact List (SEE APPENDIX B).
  - Texas Secretary of State (SOS)
  - Texas Department of Information Resources (DIR)
  - Cybersecurity Service Provider
  - Law Enforcement
  - Legal Counsel
  - Government Officials


## STEP 4: NOTIFY AND ASSEMBLE THE INCIDENT RESPONSE TEAM

- The Election Administrator, Loretta Mason should immediately contact and gather the Incident Response Team, a cross-functional team composed of organization's stakeholders and Incident Handlers, the individuals pre-assigned to perform incident response tasks as defined in the Incident Response Team Roles and Responsibilities chart. (SEE APPENDIX C)
- As soon as the Incident Response Team is notified, each person identified as an Incident Handler must receive an Incident Handler's Log and Report template (SEE APPENDIX A) to begin recording his or her activities and observations.
- Incident Handlers will submit their completed Incident Handler's Logs and Reports to the Incident Response Commander who will compile them into the master Incident Report at the conclusion of the incident.




STEP 5: ANALYZE THE EVENT FOR SCOPE AND START REPORT

- Barry Tate, IT Specialist must analyze the incident to confirm the full scope and document the discovered facts in the Incident Handler's Log (SEE APPENDIX A):
  - Source of the issue (outside actor, insider)
  - Motive (Malicious or accidental)
  - List of affected or involved resources (network, systems, data, software, credentials, business processes)
  - The type of data that is involved (sensitive, confidential or other) and what is the quantity of data
  - People affected by the issue (number of people, internal or external, departments)
  - The type of incident:
    - Ransomware
    - Malware
    - Denial of Service
    - Malicious Code
    - Improper Usage
    - Scans/Unauthorized Access
    - Phishing
- Loretta Mason, Election Administrator should determine the severity of the incident as defined in the Incident Severity Classification System in Table 1.

TABLE 1: INCIDENT SEVERITY CLASSIFICATION SYSTEM

SEVERITY CLASSIFICATION	VOTERS AFFECTED	# OF DEPARTMENT USERS IMPACTED	IMPORTANT INDIVIDUALS IMPACTED	APPLICATIONS & SYSTEMS CRITICAL TO OPERATIONS	NON-CRITICAL APPLICATIONS & SYSTEMS
CRITICAL 	Greater Than 50%	Greater Than 25%	County Judge, Elected Officials, Election Administrator	Unavailable, Infiltrated or Data Loss Suspected	Infiltrated or Data Loss Suspected



HIGH 	25% To 50%	15% To 25%	Department Heads, County Officials	Impaired but Available	Unavailable
MODERATE 	10% To 25%	10% To 15%	-	Issues Experienced	Impaired but Available
LOW 	Less Than 10%	Less Than 10%	-	-	Issues Experienced

### STEP 6: SET UP A COMMAND CENTER

- The Election Administrator, Loretta Mason, Barry Tate, IT specialist and Bryan Murff, Emergency Management Coordinator must set up an Incident Response Command Center in the 3<sup>rd</sup> floor election room. Access to the room should be controlled by keeping the door locked and providing keys to the Incident Response Team only. If electronic access can be granted to the Response Command Center, make sure that only those staff involved in the response have badge controlled access to the room.

### STEP 7: ASSEMBLE INCIDENT RESPONSE RESOURCES

- The Election Administrator, Loretta, Barry Tate, IT specialist and Bryan Murff, Emergency Management Coordinator must gather the resources needed to conduct Incident Response operations in the Command Center as specified in the Incident Response Resource List in Table 2.

**TABLE 2: INCIDENT RESPONSE RESOURCE LIST**

1. Printed copy of the Election Written Information Security Program (WISP). The printed version of the Election WISP is located 3<sup>rd</sup> floor election room. These documents should be placed in a central location in the Incident Response Command Center to remain easily accessible to the Incident Response Team for quick reference.
  - Election Incident Response Plan
  - Election Information Security Policy
    - Asset Inventory
    - Topology Diagram of the Network

- Data Inventory
  - Continuity of Operations Plan
- 2. 10 printed copies of the Incident Handler's Log and Report (APPENDIX A). The copies are stored with printed version of the Election WISP located *elections office.*
- 3. Instructions for specific technical activities
  - How to run AV scanning
  - How to capture network packets
  - How to restore data from backups
- 4. White boards and/or projection equipment to provide visibility of Incident Response activity and progress to the team
- 5. Printed Emergency Contact List of personnel and vendors with names, titles, mobile numbers and email addresses (APPENDIX D). The copies are stored with the printed version of the Election WISP located *3<sup>rd</sup> floor election room.*
- 6. Spare equipment if primary hardware is quarantined due to the attack
  - Cell phones for alternative communications
  - Three laptops, tablets or other non-affected devices
  - One server, if applicable
  - Cables
  - Basic Networking Equipment – switches, modems, routers etc.
  - Toolkit with all relevant parts and tools necessary to effect repairs
- 7. Blank USB Drives
- 8. Blank backup storage units with encryption capabilities
- 9. Digital backup devices (e.g. hard disk cloners) and software to create disk images, capture memory state of hosts, preserve log files, and save other relevant incident data
- 10. 10 printed copies of Communication Plan Forms (APPENDIX E)
- 11. Evidence gathering accessories
  - Hardbound notebooks
  - Digital cameras
  - Audio recorders
  - Evidence / Chain of Custody Log (APPENDIX F)
  - Evidence storage bags/tags/tape to preserve evidence for possible legal actions or insurance requirements

12. Written statement listing the circumstances under which the Election Authority will or will not pay a ransom in the event of a ransomware attack. When making this plan, you must consult the entity within your county or city who controls the budget under which you operate.

#### STEP 8: INITIATE THE CONTINUITY OF OPERATIONS PLAN

- Refer to the Continuity of Operations Plan (COOP) in the Election WISP

#### STEP 9: WORK WITH THE IT STAFF TO CONTAIN THE DAMAGE

- Possible incident containment activities include, but are not limited to:
  - Disconnect infected devices and systems from the network
  - Segregate affected systems
  - Reroute network traffic to avoid possible infection from the network
  - Filter or block the attack
  - Refer to the Election Authority's written statement regarding the pre-determined response to handling ransomware demands.
  - Continue to investigate scope and additional infected systems and devices
  - Update scanning software to include the virus signature and scan all other devices for possible infection
  - Change passwords for compromised credentials
  - Erase infected drives and remove the virus, malicious code, hacker tools and inappropriate material
  - Preserve and collect all evidence for insurance or law enforcement investigation and maintain an Evidence / Chain of Custody Log (APPENDIX F)

#### STEP 10: NOTIFY THE INSURANCE PROVIDER, IF APPLICABLE

- Loretta Mason, Elections Administrator should contact Jennifer Stacy, County Auditor to contact the Cybersecurity Insurance Provider, if applicable, when a cybersecurity incident is confirmed and coordinate with the company to provide the necessary information, documentation and approvals.
- The Cybersecurity Insurance Policy provides coverage for:
  - Breach Costs (including Computer Forensics, Notification, Call Center, Identity Protection Services, Crisis Management and Public Relations)
  - Penalties (includes all amounts awarded in a Regulatory Proceeding)



- PCI Fines and Assessments
- Cyber Extortion Costs
- Business Interruption Costs
- Data Recovery Costs

INSURANCE PROVIDER	
CARRIER NAME	TAC
POLICY NUMBER	CAS-1830-20230101-1
PRIMARY CONTACT NUMBER	Todd Kissel
INCIDENT HOTLINE NUMBER	800-456-5974
AUTHORIZED COUNTY CONTACT	Jennifer Stacy
SECONDARY AUTHORIZED COUNTY CONTACT	Robyn Klysen

#### STEP 11: INITIATE THE INTERNAL COMMUNICATIONS PLAN

- The designated Incident Response Team Communications Director must develop and disseminate information about the incident to the internal staff using the Communications Plan. (APPENDIX E).
- The Incident Response Team must maintain secure communications with employees and other internal stakeholders during an incident, limiting communications regarding the details of the incident on a need-to-know basis.
- Internal communications should consist of:
  - Instructions to internal staff regarding steps to take to protect their devices or repair devices affected by the incident
  - Notification to state government leadership regarding the incident
  - Information to other state and/or federal agencies
- Notification details should include:
  - What happened?
  - When did the incident occur and/or when was it detected?
  - How was it detected?

- What data was potentially compromised?
- How much data was compromised?
- Whose data was compromised?
- Why the recipient is being notified?
- What steps were/are being taken?
- What steps should individuals take?
- If a service is being offered to affected individuals, how long do they have to enroll?
- Anticipated next steps, if any
- Who to contact for additional information (Contact name, number, hours of availability, website, hotline, email address, etc.)
- Signature (The letter should be signed by an official with responsibility over the compromised data)

#### STEP 12: INITIATE THE EXTERNAL COMMUNICATIONS PLAN

- The designated Incident Response Team Communications Director must develop and disseminate information about the incident to the external stakeholders in alignment with data security policies associated with the Election Data Classification System.
- External communications should consist of:
  - Announcements to third-party vendors
  - Press release to the media
  - A press briefing if the incident is deemed critical
- Elements of a press release and press briefing should include:
  - What happened
  - Resolution
  - Notification has occurred
  - Who is affected/not affected
  - What specific types of personal information are involved
  - What are the (brief) details of the incident
  - Whether or not evidence indicates data has been misused
  - Expression of regret and steps being taken to prevent similar incidents from happening again
  - Major actions taken
  - Where to go for more information

### STEP 13: RECOVER THE ASSETS AND DATA

- The Incident Response Team must work with key IT staff to perform recovery processes. Only personnel with expert technical training should engage in the recovery activities. Recovery activities include but are not limited to:
  - Rebuilding and reimaging the devices and systems from scratch
  - Loading backed-up data to the devices and systems
  - Replacing compromised files with clean versions
  - Scanning for traces of malicious software, hacker tools or code
  - Apply all recent patches
  - Testing the devices and systems before reconnecting to the network

### STEP 14: DOCUMENT THE INCIDENT IN A CYBERSECURITY INCIDENT REPORT

- If an incident is detected, create a report using the information gathered in the Incident Handler's Logs (APPENDIX A) that includes:
  - How the incident was detected
  - The scope, severity and impact of the incident
  - How the incident occurred
  - The people and departments affected
  - Who was notified and when
  - The steps taken to contain the incident
  - The incident analysis results
  - Internal and external communication
  - Recovery activities
  - How this incident type can be prevented in the future
  - Lessons Learned

### STEP 15: IDENTIFY LESSONS LEARNED AND UPDATE THE PLAN

- Upon closure, review each incident via a "lessons-learned" aka "After Actions Review" meeting and document it in the Incident Handler's Log (SEE APPENDIX A). Shouldn't the lessons learned be documented in a revised version of the Incident Response Plan?
- Lessons learned will be integrated into the Cybersecurity Incident Response Plan to improve responses to a future incident, should one occur.
- Access to "After Actions Review" documentation is restricted to Incident Response Team members unless the team determines the report should be released to other approved individuals.

## STEP 16: COLLECT AND SUBMIT EVIDENCE

- All evidence must be gathered including infected technology, information about the incident and the Evidence / Chain of Custody Log (APPENDIX F) and submitted to the insurance company, forensics team or law enforcement agency as required.







APPENDIX B: INCIDENT NOTIFICATION PRIORITY CONTACT LIST

Organization	Name	Title	Phone	Email	When to Contact and Why
Office of the Texas Secretary of State (SOS)	Christina Adkins	Director of Elections	512-463-5650 Ext. 1	elections@sos.texas.gov	IMMEDIATELY after a valid incident is confirmed in order to engage in coordinated response
Texas Department of Information Resources (DIR)			512-475-4700	Security-alerts@dir.texas.gov	After valid incident is confirmed for assistance with technical aspects of response
Cybersecurity Service Provider	Barry Tate	IT Specialist	903-261-7864	itadmin@co.panola.tx.us	
Law Enforcement	R.C. Cutter Clinton	Sheriff	903-263-8469	<a href="mailto:cutter.clinton@co.panola.tx.us">cutter.clinton@co.panola.tx.us</a>	After valid incidence
Legal Counsel	Danny Buck Davidson	County Attorney/District Attorney	903-693-0311	danny.davidson@co.panola.tx.us	After valid incidence
Government Officials	Rodger McLane	County Judge	903-693-0391	rodger.mclane@co.panola.tx.us	After valid incidence
EI ISAC/MS ISAC	Any member that answers	Member	1-866-787-4722	soc@cisecurity.org	After incident facts have been collected to share information that helps other agencies guard



					against similar attacks.
--	--	--	--	--	--------------------------

APPENDIX C: INCIDENT RESPONSE TEAM ROLES AND RESPONSIBILITIES

IR TEAM ROLE		RESPONSIBILITIES	PERSON ASSIGNED
INCIDENT HANDLERS	IT STAFF, IT VENDOR OR CYBERSECURITY VENDOR	<ul style="list-style-type: none"> <li>• Provide technical expertise as needed</li> <li>• Serve in an on-call, 24/7 capacity in the event of an incident</li> <li>• Provide documentation as requested concerning the technical nature of the incident</li> <li>• Document activities in an Incident Handler's Log and Report</li> </ul>	Name: Barry Tate Title: IT specialist Phone: 903-261-7864 Email: itadmin@co.panola.tx.us Date Assigned:

<p>INCIDENT HANDLER</p>	<p>INCIDENT RESPONSE COMMANDER: <i>LORETTA MASON,</i> <i>EA</i></p>	<ul style="list-style-type: none"><li>• Function as the central point of contact and the lead for all incidents</li><li>• Initiate and coordinate incident response activities</li></ul> <p>Start the Cybersecurity Incident Handler’s Log and Report as soon as an incident is confirmed and update the report throughout the incident, documenting the incident response activities, timeline, key decision points and rationale, and progress of the remediation efforts</p> <ul style="list-style-type: none"><li>• Coordinate the containment and remediation of the incident with the IT Staff</li><li>• In conjunction with Legal Counsel, ensure that evidence is appropriately gathered, preserved and the chain of custody is maintained</li><li>• Coordinate the internal and external communication plans.</li><li>• After the incident has been remediated, compile copies of the Incident Handlers’ Logs from other team members and add relevant information to the master report. Complete the report and submit it to the Texas Secretary of State’s Office.</li><li>• Conduct a “Lessons Learned” review after every incident and update the Cybersecurity Incident Response Plan</li></ul>	<p>Name: Loretta Mason Title: EA Phone: 903-754-7275 Email: <a href="mailto:lmason@co.panola.tx.us">lmason@co.panola.tx.us</a> Date Assigned:</p>
-------------------------	---	---	---

INDICENT HANDLER	Loretta Mason, EA	<ul style="list-style-type: none"> <li>• Serves as the central source of information</li> <li>• Keep the Incident Response Team consistently informed of important media activities</li> <li>• Develops talking points for leadership and anyone communicating with the public and media</li> <li>• Creates press releases for the media</li> <li>• Briefs the press on relevant incident information in accordance with the Election Data Classification System in the Election Information Security Policy</li> <li>• Documents activities in an Incident Handler's Log and Report</li> </ul>	Name: Loretta Mason Title: EA Phone: 903-693-0370 Email: lmason@co.panola.tx.us Date Assigned:
STAFF MEMBERS	<ul style="list-style-type: none"> <li>• Execute the Continuity of Operations Plan</li> <li>• Participate in "Lessons Learned" discussions</li> </ul>	Name: Kelsey Gates Title: Assistant Phone: 903-693-0370 Email: Kelsey.lake@co.panola.tx.us Date Assigned:	
COUNTY AUTHORITY LEADERSHIP: <u>[COMMISSIONER OR DESIGNEE]</u>	<ul style="list-style-type: none"> <li>• Stay informed of the incident response progress and advise regarding the operational impact of containment and recovery decisions</li> <li>• Coordinate requirements and engagement with the cybersecurity insurance provider, if applicable</li> </ul>	Name: Loretta Mason Title: Elections Administrator Phone: 903-693-0370 Email: lmason@co.panola.tx.us Date Assigned:	
LEGAL COUNSEL	<ul style="list-style-type: none"> <li>• Engage and supervise outside counsel when warranted</li> </ul>	Name: Danny Buck Davidson Title: DA, County Attorney	



	<ul style="list-style-type: none"> <li>• Report incidents to the relevant insurance broker and/or carrier as necessary</li> <li>• Assesses the extent of legal steps needed (such as the need to direct the forensic investigation)</li> <li>• Oversees the preservation of evidence, and that the chain of custody is maintained</li> <li>• Advises the Incident Response Team on all legal, regulatory and contractual requirements related to the incident, including any obligation to notify external organizations, clients, business partners, affected individuals or regulatory agencies</li> <li>• Determines public reporting obligations</li> <li>• Provides advice on all communications (both internal and external) related to the incident, including any law enforcement authorities</li> <li>• Provides legal support related to an incident (e.g. prosecution of a suspect, handling of lawsuits arising from an incident, developing contracts or other binding agreements for external services)</li> </ul>	<p>Phone: 903-693-0311</p> <p>Email: danny.davidson@co.panola.tx.us</p> <p>Date Assigned:</p>
<p>HUMAN RESOURCES LIAISON</p>	<ul style="list-style-type: none"> <li>• Ensures that employees understand how to respond to inquiries from external parties and understand the County's confidentiality obligations regarding the incident</li> <li>• Provides advice regarding employee relations</li> <li>• Assists with any disciplinary proceedings as appropriate (e.g. if an employee is suspected of causing an incident)</li> </ul>	<p>Name: Joni Reed</p> <p>Title: Treasurer</p> <p>Phone: 903-693-0326</p> <p>Email: joni.reed@panola.tx.us</p> <p>Date Assigned:</p>



APPENDIX E: COMMUNICATIONS PLAN

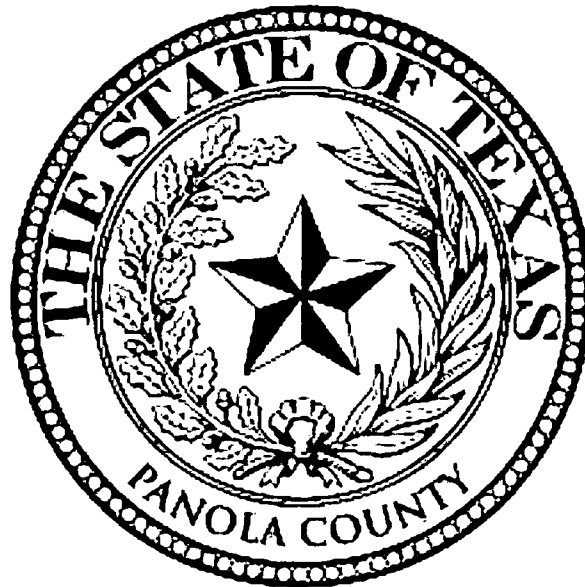
Audience	Frequency	Method	Purpose of the Communication	Person Responsible for the Communication	Date & Time
IT Team Members Barry Tate	Every hour	Text	To communicate what has happened and what our plan is.	Loretta Mason Barry Tate Bryan Murff	
General Counsel Danny Buck Davidson	As soon as incidence happens	Text	To communicated what has happened and what our plan is.	Loretta Mason Barry Tate Bryan Murff	
Human Resources Joni Reed	As soon as incidence happens	Text	To communicate what has happened and what our plan is.	Loretta Mason Barry Tate Bryan Murff	
Internal Audit Jennifer Stacy	As soon as incidence happens	Text	To communicate what has happened and what our plan it.	Loretta Mason Barry Tate Bryan Murff	
Crisis Management Team Loretta Mason Barry Tate Bryan Murff	As soon as incidence happens	Text	To communicate what has happened and what our plan is.	Loretta Mason Barry Tate Bryan Murff	
Leadership/Management Loretta Mason	Will be the first to know and will communicate to everyone	Text	To communicate what has happened and what our plan is.	Loretta Mason Barry Tate Bryan Murff	



Employees Kelsey Gates	As soon as Incidence happens	Text	To communicate what has happened and what our plan is.	Loretta Mason Barry Tate Bryan Murff	
Commissioners Court Rodger McLane Billy Alexander David Cole Craig Lawless Dale LaGrone	As soon as incidence happens	Text	To communicate what has happened and what our plan is.	Loretta Mason Barry Tate Bryan Murff	
Outside Counsel Collin Underwood	Once we determine what we need to do	Text	To communicate what has happened and what our plan is.	Loretta Mason Barry Tate Bryan Murff	
Law Enforcement R.C. Cutter Clinton, Sheriff	Once we determine what we need to do	Text	To communicate what has happened and what our plan is.	Loretta Mason Barry Tate Bryan Murff	
Cyber Insurance Carrier TAC	Once a incidence happens	Phone call	To communicate what has happened and what our plan is.	Loretta Mason Barry Tate Bryan Murff	



*PANOLA COUNTY  
ELECTIONS  
VENDOR RISK  
MANAGEMENT POLICY*



## DOCUMENT MANAGEMENT

The Vendor Risk Management Policy must be reviewed at least once per year or more frequently if state or federal legislation mandates new election security requirements. It should also be reviewed as new cyberthreats emerge, or when new vendors or organizational changes require plan updates between yearly reviews.

Maintain a record of all policy reviews in the Policy Review Log to validate that the Vendor Risk Management 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						
Drafted By		Signature		Date		
Approved By		Signature		Date		
<b>REVIEW AND REVISION LOG</b>						
<b>REVIEW SCHEDULE:</b> General Election Years: December after elections Legislative Session Years: July after SOS Law Conference						
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

---

INTRODUCTION..... 5

SCOPE..... 5

GOVERNANCE ..... 6

    POLICY 4: SUPPLY CHAIN RISK MANAGEMENT..... 6

Vendor Risk Management Policy and Assessment Survey..... 8

    VENDOR INSTRUCTIONS..... 8

**CONFIDENTIAL INFORMATION WARNING**

This document contains information about the security of Panola County Elections 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 Panola County Elections Confidential, and cannot be reproduced, redistributed in any way, shape or form without prior written consent from *Panola County Elections*.

## INTRODUCTION

---

*Panola County Elections* uses information technology to manage and deliver services to our citizens and voters. The critical role that technology plays in election operations drives the need to protect the confidentiality, privacy, integrity, and availability of information and communications systems from cyberattack or other disruptive events. By evaluating the key cybersecurity practices implemented by third-party vendors, *Panola County Elections* is able to ensure that security is at the foundation of all operations.

The **Vendor Risk Management Policy** is presented in the form of an assessment survey to provide a way to evaluate vendor cybersecurity practices and technologies. This helps to ensure that risks associated with outsourcing services and utilizing technology provided by third-party suppliers are understood and reduced where possible.

Each vendor must include a statement specifying that the vendor agrees to provide information in response to the Election Authority's ongoing cybersecurity reviews through the survey process.

## SCOPE

---

This Policy is used to assess vendors that provide election services that may include, but are not limited to:

- Election management systems
- Ballot creation, printing, and programming services
- Ballot marking devices (BMDs) and direct-recording electronic (DRE) equipment used to capture votes
- Tabulation software systems
- Ballot scanner equipment
- Voter registration software systems
- Inventory management systems



- ePollbook technologies and management platforms
- Document scanning and management systems
- Website hosting platforms and providers
- Email hosting providers
- Election night reporting systems
- Other technology vendors and managed service providers

The Policy encompasses technology and ongoing services arrangements, including remote maintenance and access requirements, to help understand the full scope of third-party supplier risks and the need for risk assessments.

## GOVERNANCE

---

The *Loretta Mason* must ensure that vendors complete the assessment survey portion of the [Vendor Risk Management Policy](#). Vendors are required to remediate any issues identified during the assessment process before working with Loretta Mason. If circumstances make it necessary to consider an exception, the *Loretta Mason* is responsible for reviewing the risk and making a determination as to whether or not the vendor is allowed to implement an alternate practice or can be exempt from the requirement if the risk is determined to be accepted by the Loretta Mason.

The Vendor Risk Management Policy enables Panola County Elections to meet requirements outlined in the Election Information Security Policy, specifically Policy 4: Supply Chain Risk Management.

### 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 and updated, if needed, at least yearly as part of the Policy 1 Election WISP annual review requirement.

- Vendor risk assessment should be conducted annually by communicating with vendors to see if any significant changes to their networks, technologies, or business processes have recently occurred and by staying informed of cyberthreats that could affect vendors via the Information Sharing and Analysis Center (ISAC) 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 facilities, and vendors who regularly work in our facilities are required to have identification badges that are not capable of opening doors or accessing secure areas.
- Vendor risk assessment will be evaluated annually as part of the Election WISP review described in the Policy.

The section that begins on the next page should be provided to vendors. Request that the vendor complete the survey with as much detail as possible.

## Vendor Risk Management Policy and Assessment Survey

---

### VENDOR INSTRUCTIONS

It is requested that *the Vendors* provide descriptions and examples, where applicable, that illustrate how your organization performs cybersecurity functions and otherwise enables capabilities that follow the Panola County Elections Vendor Risk Management Policy. Because your organization interacts with critical aspects of the supply chain and business process enablement for Panola County Elections, your capabilities factor into the County's risks that may potentially include disclosure of voter registration information, invalidation of voter registration information, disruptions to the voting process, invalidation of the results of an election, or contribute to speculation about the validity, fairness, or accuracy of the election process.

Please complete the profile fields in the following assessment survey, and provide specific information related to how your organization supports Panola County Elections.

This assessment survey is derived from the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). The survey items provided are based upon an organizational risk scoring that evaluates the functionality that the services or products under consideration will provide. Scoring is conducted based upon factors that include the business criticality of the services and products; the types of data that will be stored, processed, transmitted or accessed via the service or products; and other risk factors such as legal and reputational risks to the organization.

Further information about the NIST Cybersecurity Framework can be found by visiting: <https://www.nist.gov/cyberframework>. This assessment survey is intended to provide information that will permit the Election Authority to evaluate the controls and environment that relate to the service or product under consideration. It is not Panola County Elections recommendation or requirement that the company completing the assessment survey base its controls or security functions on the NIST Cybersecurity Framework.

### COMPANY INFORMATION

Company Name	Election Systems & Software (ES&S)
Name of Parent Company	N/A
Primary Business Address	11208 John Galt Blvd Ste 200, Omaha NE 68137
Address of Production Data Center	11208 John Galt Blvd Ste 200, Omaha NE 68137
Address of Backup Data Center	TierPoint Datacenter 11425 S 84th Street, Papillion, NE 68046
Other Addresses of Facilities Used in Providing Services or Products	<ul style="list-style-type: none"> <li>- Richardson, TX, 1217 Digital Drive, Suite 180, 75081, Election Services</li> <li>- Rockford, IL, 929 South Alpine #301, 61108, Software Development Office</li> <li>- Birmingham, AL, 252 Oxmoor Court, 35209, Printing and Services Office and Warehouse</li> <li>- Jackson, MS, 5738 Highway 80 West, 39209, Sales Office,</li> <li>- Bowie, MD, 4931 Telsa Drive, 20715, Warehouse and Services</li> <li>- Hatfield, PA, Unit A, 7 Church Road, 19440, Sales Office</li> <li>- Midland, TX, 3400 West Loop, 250 North, 79707, Storage Only</li> <li>- Columbus, OH, 5341 North Hamilton Rd, 43230, Storage Only</li> <li>- Omaha, NE, 9992 F Street, 68127, Warehouse</li> <li>- Vorhees, NJ, Nine Point Property, 300 Somerdale Rd, 08053, Sales Office</li> <li>- LaVista, NE, Pivot/EDM, 12202 Cary Circle, 68128, Warehouse</li> <li>- Omaha, NE, 4220 South 102nd Street, 68127, Warehouse and Equipment Preparation</li> <li>- LaVista, NE, 8619 South 137th Circle, 68137, Warehouse</li> </ul>

### RESPONDER INFORMATION

Company Single Point of Contact Name	Christopher Wlaschin
--------------------------------------	----------------------



Title	Senior Vice President and CISO
Email	chris.wlaschin@essvote.com
Phone	402-938-1450 (o) 402-525-6759 (c)

### ASSESSMENT SURVEY ITEMS

#### IDENTIFY

1	Describe how your organization actively tracks and manages authorized hardware devices and systems to ensure that unauthorized devices and systems are identified and prevented from gaining access.	ES&S utilizes automated workflow process tools and a centralized ticketing system to track authorized hardware on its corporate network. Devices are catalogued in the ticketing system upon receipt and removal from the network. Each time a device attempts to connect to the network, MAC address filtering combined with Active Directory user authentication verification is conducted before an authorized device is connected to the network. Routine scans of the network are conducted to detect unauthorized devices. Company IT security policy prohibits the connection of unauthorized devices to the network. Only authorized and trained IT service center personnel are allowed to make changes to the network hardware inventory and those changes are tracked by a change control plan which is reviewed by management.
2	Describe how your organization actively tracks and manages authorized software to ensure that unauthorized software and applications are identified and prevented from installation or execution.	ES&S uses a gold disk image to create standard network endpoint software deployments. This image contains licensed versions of all commercial software that our workforce requires to conduct business. Users who desire additional software must initiate a service request ticket to the IT service center and once approved will then add authorized software to the user device. On the server-side ES&S creates all images used in our server environment. We are a VMware shop so we create and deploy our own server images across all of the production, test, QA and development server environments. Each server environment is separated from the

		<p>production environment and each required unique user authentication controls.</p>
<p>3</p>	<p>Describe how your organization tracks and manages authorized data flows, application programming interfaces (APIs), and the extraction of data to ensure unauthorized access and removal of data does not occur.</p>	<p>The ES&amp;S public facing web presence is hosted by a third-party website hosting service in another state and has no physical or logical connection to the ES&amp;S corporate IT environment. There is no data exchange from the public facing web presence and ES&amp;S corporate IT. A contact page collects questions and forwards them to our marketing department via secure email.</p> <p>ES&amp;S customer data is segregated from the corporate IT environment by physical and logical controls. All customer data is encrypted at rest and in motion using FIPS 140 standard encryption. A limited number of ES&amp;S personnel have access to customer data and all actions related to customer data are logged and available for review.</p>
<p>4</p>	<p>Describe how information resources are classified and categorized to ensure appropriate controls for protection and timely recovery, as well as for retention and planned destruction.</p>	<p>ES&amp;S has a Data Protection Policy managed by a standing data protection committee. The policy sets forth the data class, business impact, examples, and protections for each level or class. Examples of protection level 3 (highest) include data that creates extensive "shared-fate" risk between multiple sensitive systems, e.g., enterprise credential stores, backup data systems, and central system management consoles. Examples of protection level 2 include data that could be used to identify individuals, harm ES&amp;S or its employees, or expose confidential or valuable information including data containing personally identifiable, sensitive, secret, or proprietary information. Examples of protection level 1 include information intended for release only on a need-to-know basis, including personal information not otherwise classified as Level 0, 2 or 3, and data protected or restricted by contract, grant, or other agreement terms and conditions, e.g., Data guardians have been designated for each</p>



		<p>employee group to administer the policy. All employees have been given this policy and are accountable for its use.</p>
<p>5</p>	<p>Describe how your organization ensures that personnel have the required expertise and skills to perform their job duties and how they are trained on an ongoing basis to maintain required skills.</p>	<p>ES&amp;S has a thorough pre-employee screening process that matches prospective employees to the jobs they are applying for. New employees are evaluated during the first-year probation period to ensure that the required expertise and skills for the position are in fact present. Software developers, hardware engineers, programmers and IT employees obtain training and certification where appropriate for their skill set and are encouraged to pursue ongoing training to maintain required skills.</p>
<p>6</p>	<p>Describe your organization's processes for identifying vulnerabilities within the information technology environment and network infrastructure and how remediation is performed to minimize exposure to threats and attackers.</p>	<p>ES&amp;S is a member of the MS-ISAC, EI-ISAC and IT-ISAC which allows us to receive cyber threat information feeds from these organizations who are connected to DHS and the US intel community generating these feeds. ES&amp;S also subscribes to all OEM vulnerability alerts so that we receive notification from the manufacturer of the COTS equipment we use. ES&amp;S employs an internal vulnerability assessment team that takes the alerts from the various feeds and reviews them for applicability to our systems as well as any recommended patches. ES&amp;S follows the CVSS vulnerability rating system and patches critical and high vulnerabilities immediately after testing. Medium, low and informational vulnerabilities are patched as time and resources allow. ES&amp;S conducts internal vulnerability scans of our network environment using Nessus and other scan tools. ES&amp;S contracts with an external 3rd party security company to scan our corporate IT environment, and we contracted with another 3rd party security company to conduct independent vulnerability assessments of our corporate IT environment.</p>



<p>7</p>	<p>Describe how your organization tests the overall strength of defenses and simulates the actions of attackers, including penetration tests that are conducted periodically.</p>	<p>ES&amp;S employs multiple measures to monitor ongoing security threat changes and respond to evolving threats. As stated elsewhere in this document, ES&amp;S has installed five Albert sensors in the voter registration environments we host for customers.</p> <p>ES&amp;S has published a Coordinated Vulnerability Disclosure Program for our public facing assets including our corporate network and web presence that is in use and productive.</p> <p>We have DHS CISA cyber hygiene teams scan our public facing internet presence weekly looking for vulnerabilities, and ES&amp;S works with multiple federal, state and local entities to be informed of and manage security risks to our hardware, software and services.</p> <p>ES&amp;S has two separate 3rd party security entities monitoring our internal network looking for indicators of compromise.</p> <p>We subscribe to multiple cyber threat feeds that allow us to assess and react if necessary, to any security threat to our systems or our customers. These cyber threat feeds originate from the U.S. Intelligence community, U.S. law enforcement, the U.S. Department of Homeland Security, the Multi-State Information Sharing and Analysis Center (MS-ISAC), the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), and the National Cybersecurity Communications and Information Center (NCCIC).</p> <p>ES&amp;S uses the same common vulnerabilities and exposures (CVEs) system that the federal government uses to rank cyber risk and assign corresponding resources to mitigate those risks where applicable to ES&amp;S products.</p>
<p>8</p>	<p>Describe how your organization assesses, addresses, and accepts cybersecurity risks.</p>	<p>In 2018 ES&amp;S formed a Corporate Risk Management Team chaired by the SVP of Security/CISO and includes company executives (CEO, CFO, SVP's), general counsel and other</p>

subject matter experts who document and evaluate risks to the business including IT security risks. This group meets quarterly. Broad categories of risk include operations, corporate IT, product security, manufacturing, physical security, staffing, and supply chain. These categories of risk are reviewed monthly and prioritized based on severity and likelihood of applicability then scheduled for the application of resources. Where appropriate, risks are mitigated through managed and monitored actions. Risks can be deferred or accepted if the situation calls for it. Risk is reported to the Board of Directors on an as-needed basis.

The nature of elections makes them vulnerable to a range of security threats against participants, infrastructure, information and materials. Effective election security must draw on information and expertise from multiple arenas. A high level of communication and coordination among the agencies responsible for the administration and security of an election is a significant advantage. Neither can security analysis and planning be effective when it occurs only in a period shortly before the electoral process starts, nor depend solely on reactive strategies. Anticipating and pre-empting security risks, mitigating their impact or probability of occurrence, is a strategic endeavor of both the electoral authorities and their security partners. The following table and accompanying narratives describe the major risks, severity, likelihood, mitigation and residual risk.

		<table border="1"> <thead> <tr> <th>Risk</th> <th>Severity</th> <th>Likelihood</th> <th>Mitigation</th> <th>Residual Risk</th> </tr> </thead> <tbody> <tr> <td>Formal security program</td> <td>Medium</td> <td>Low</td> <td>Plan a CISO, establish program</td> <td>Low</td> </tr> <tr> <td>Software development</td> <td>High</td> <td>Medium</td> <td>Enforce secure dev development by qualified developers</td> <td>Medium. User requires constant attention and testing</td> </tr> <tr> <td>Hardware development</td> <td>High</td> <td>Medium</td> <td>Use ISO processes and include complete QA, QC every step</td> <td>Low</td> </tr> <tr> <td>Physical security</td> <td>Medium</td> <td>Medium</td> <td>Enforce physical security controls on in plant and movement</td> <td>Medium</td> </tr> <tr> <td>Personnel security</td> <td>Medium</td> <td>Medium</td> <td>Background checks for all employees, contractors, temps and interns</td> <td>Low</td> </tr> <tr> <td>Insider threat</td> <td>High</td> <td>High</td> <td>Establish Insiders with training relationships with DHS, ISAC, the IC and other entities</td> <td>Medium. Data sharing is 7 yrs and requires constant attention and monitoring</td> </tr> <tr> <td>Data security</td> <td>High</td> <td>High</td> <td>Establish data governance and processes to protect sensitive data</td> <td>Medium. Data security requires constant monitoring of mistakes</td> </tr> </tbody> </table> <p>As your election vendor and security partner, ES&amp;S takes cybersecurity very seriously, as evidenced by our adding a Senior Vice President of Security and Chief Information Security Officer (CISO) to the team (the only major manufacturer to do so). Chris Wlaschin is a Certified Information System Security Professional (CISSP) with 20+ years' experience in cybersecurity. Before joining ES&amp;S, he served as the Chief Information Security Officer for the Department of Health and Human Services (HHS) in Washington, D.C. where he oversaw cybersecurity efforts for the Department. He has held other senior cybersecurity leadership positions in both the public and private sector including the Department of Defense, Department of Veterans Affairs, National Research Corporation, the University of Nebraska and the Defense Intelligence Agency. He is a graduate of both Southern Illinois and Northern Illinois. Having a C-level CISO on board benefits our customers by bringing his security leadership and experience to everything we do from the design of our equipment to our ongoing support of elections in the field.</p>	Risk	Severity	Likelihood	Mitigation	Residual Risk	Formal security program	Medium	Low	Plan a CISO, establish program	Low	Software development	High	Medium	Enforce secure dev development by qualified developers	Medium. User requires constant attention and testing	Hardware development	High	Medium	Use ISO processes and include complete QA, QC every step	Low	Physical security	Medium	Medium	Enforce physical security controls on in plant and movement	Medium	Personnel security	Medium	Medium	Background checks for all employees, contractors, temps and interns	Low	Insider threat	High	High	Establish Insiders with training relationships with DHS, ISAC, the IC and other entities	Medium. Data sharing is 7 yrs and requires constant attention and monitoring	Data security	High	High	Establish data governance and processes to protect sensitive data	Medium. Data security requires constant monitoring of mistakes
Risk	Severity	Likelihood	Mitigation	Residual Risk																																						
Formal security program	Medium	Low	Plan a CISO, establish program	Low																																						
Software development	High	Medium	Enforce secure dev development by qualified developers	Medium. User requires constant attention and testing																																						
Hardware development	High	Medium	Use ISO processes and include complete QA, QC every step	Low																																						
Physical security	Medium	Medium	Enforce physical security controls on in plant and movement	Medium																																						
Personnel security	Medium	Medium	Background checks for all employees, contractors, temps and interns	Low																																						
Insider threat	High	High	Establish Insiders with training relationships with DHS, ISAC, the IC and other entities	Medium. Data sharing is 7 yrs and requires constant attention and monitoring																																						
Data security	High	High	Establish data governance and processes to protect sensitive data	Medium. Data security requires constant monitoring of mistakes																																						
9	Describe your organization's processes for managing the development, testing, and quality assurance of applications, software,	As standard procedure, our internal security team conducts thorough and pervasive penetration testing of our hardware and software using the same modern security tools																																								



and client configurations to ensure vulnerabilities within your products are identified and remediated.

that hackers might use to make sure our equipment is secure before it ever reaches the customer. After the 2018 election, to complement our own testing, we submitted our current hardware to third-party security research firms to independently verify the security of our devices. In addition, ES&S submitted our full end-to-end voting configuration of software and hardware for testing by the Idaho National Laboratory (INL), the nation's leading center for research and development in energy, national security, science and environment, to perform third-party independent testing of both our hardware and software to ensure the resilience and security of our voting systems.

Software developers and engineers at ES&S are credentialed in their areas of expertise. They employ secure-coding practices, and those practices are incorporated into all system development life cycle stages during the ES&S product development process. All ES&S source code is subject to internal peer review to confirm conformance to the industry standard coding conventions and is also externally reviewed during each EAC certification campaign by an EAC-accredited Voting System Test Lab chosen for each certification campaign. ES&S employs multiple testing methods including third-party penetration testing to ensure secure and reliable software and firmware. All ES&S source code is maintained within repositories resident on secure ES&S internal servers, and authenticated credentials are required to gain access to those repositories. There is no use of cloud services during any part of the ES&S product-development process.

The use of untested, uncertified hardware or software can put election jurisdictions at risk. ES&S products are EAC-certified and are built to all federal standards, including NIST security protocols and standards and CIS Critical Security

Controls. All ES&S systems are tested by independent laboratories that have received federal accreditation. In addition, in 2019, 2020 and 2022 ES&S submitted our end-to-end voting system to the Idaho National Labs for extensive penetration testing. Any suggestions that INL made for improvement have been incorporated into future releases.

Developers and engineers at ES&S are credentialed in their areas of expertise. They employ secure-coding practices, and those practices are incorporated into all system development life cycle stages during the ES&S product development process. ES&S software and firmware products are designed and implemented using secure-coding practices with a focus on potential security risks based upon language-specific, industry-standard coding conventions as required by the EAC Voluntary Voting System Guidelines. All ES&S source code is subject to internal peer review to confirm conformance to the industry standard coding conventions and is also externally reviewed during each EAC certification campaign by an EAC-accredited Voting System Test Lab chosen for each certification campaign. Independent unit and functional testing is also performed by the EAC-accredited Voting System Test Lab during each certification campaign to ensure proper execution and support for all declared election types. All ES&S source code is maintained within repositories resident on secure ES&S internal servers, and authenticated credentials are required to gain access to those repositories. There is no use of cloud services during any part of the ES&S product-development process.

As standard practice, each hardware and software release undergoes thousands of hours of performance testing and runs millions of test ballots along with extensive security testing after which ES&S provides a complete set of software



		<p>components to the voting systems testing labs (VSTL) for review.</p>
<p>10</p>	<p>Describe the methodology and sources your organization uses to monitor the threat landscape and obtain cybersecurity threat intelligence and indicate if your organization participates as a member of the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC).</p>	<p>First, ES&amp;S has joined two Information Sharing and Analysis Centers (ISAC): The Elections Infrastructure ISAC (EI-ISAC) and the Information Technology ISAC (IT-ISAC). Through membership in the EI-ISAC, ES&amp;S gains access to election-specific threat alerts, cybersecurity awareness and training products, and tools for implementing security best practices. Additionally, as members of the IT-ISAC, ES&amp;S is afforded opportunities to proactively analyze and share IT-focused threats to protect the nation’s voting systems and make them even more resilient to cyber-attacks. Under the leadership of the IT-ISAC, ES&amp;S is a founding member of the newly formed Elections Industry Special Interest Group (EI-SIG). The EI-SIG was formed to allow election vendors to expand information sharing concerning threats to election IT systems and engage in dialogue across sectors. ES&amp;S receives weekly threat alerts that we assess and where appropriate apply mitigating controls to our systems including the blocking of malicious IP addresses, malware infested websites, as well as phishing and related email threats.</p> <p>Second, ES&amp;S has partnered with the Election Infrastructure-Information Sharing and Analysis Center (EI-ISAC) to install five Albert network security sensors in our voter registration environments. Albert is a unique network security monitoring solution that provides continuous remote monitoring and delivery of automated alerts on both traditional and advanced network threats for state and local jurisdictions, allowing election jurisdictions and ES&amp;S to respond quickly when data may be at risk. Combined with an in-depth review conducted by expert analysts through the Center for Internet Security’s (CIS) 24/7 Security</p>



Operations Center, Albert is a fully monitored and managed service which will complement ES&S' existing robust suite of cybersecurity controls.

Third, ES&S also partners with multiple Department of Homeland Security (DHS) Critical Infrastructure Program offices including the Cybersecurity Infrastructure Security Agency (CISA) to conduct weekly cyber hygiene scans of ES&S public-facing internet presence, monitor and share cyber threat information, detect and report indicators of compromise, develop and distribute election security best practices, and raise the election security awareness of election officials and the voting public. DHS CISA weekly scans of our public facing internet presence ensure that we are alerted to and can react to any malicious activity directed towards our websites.

As a member of the MS-ISAC, EI-ISAC and IT-ISAC we receive cyber threat information feeds from these organizations who are connected to DHS and the US intel community generating these feeds. ES&S also subscribes to all OEM vulnerability alerts so that we receive notification from the manufacturer of the COTS equipment we use. ES&S has an automated process for ingesting alerts from these sources including the weekly list of high confidence IP addresses and domains associated with malware observed by MS-ISAC. We apply these threat IP's and domain addresses to our firewall blacklists within minutes of receiving them. We also review all other threat alerts sent to us by DHS, FBI and the ISAC's for applicability to our systems and apply compensating controls where appropriate.

Four ES&S senior executives have been granted US Government security clearances which enable us to attend the same classified briefings that cleared election officials attend to learn about threats to elections.

		<p>Finally, ES&amp;S relies upon an extensive network of thousands of customers across 42 states and 5 U.S. territories to share system performance, reliability and any potential cybersecurity risks they are experiencing locally with us so that we as the system manufacturer can assess any risk and where necessary apply mitigations to reduce the impact of the issues reported.</p>
<p>11</p>	<p>Describe the assurance process your organization uses to evaluate cybersecurity risks and the capabilities within your organization’s supply chain and supplier environment to mitigate them.</p>	<p>ES&amp;S has been working with the same trusted parts suppliers for more than 15 years. We conduct security assessments of their facilities, workforce, policies and procedures, and where necessary we dictate corrective actions for any deficiencies noted during site visits or documentation reviews. All our supply chain partners maintain ISO and other certification credentials. We conduct Quality Checks at each stage of the process including</p> <ul style="list-style-type: none"> <li>• Incoming parts inspection</li> <li>• Inline Mfg QA</li> <li>• Final Assemble QA</li> <li>• Omaha Inspection (FW Validation)</li> <li>• Final Order Fulfillment QA</li> <li>• On-site field services installation</li> <li>• Customer Logic &amp; Accuracy</li> </ul> <p>ES&amp;S contributed to the development of the CIS Handbook for Election Officials and has assessed our operations against the 88 controls contained therein.</p> <p>ES&amp;S voting systems are produced in ISO-9001 manufacturing facilities. The entire voting system is managed by a secure engineering change order control process. This includes all components and suppliers. Changes to the voting system follow a formal closed-loop process and must be internally and externally reviewed, verified, tested and approved before they can be incorporated. Every unit is individually serialized for complete traceability. ES&amp;S also conducts thorough security reviews of our supply chain including supply chain risk</p>



		<p>assessments based on NIST Cybersecurity Framework (CSF) Version 1.1 which includes on-site visits of our suppliers to ensure that every component is trusted, tested and free of defects. All tabulation software is produced and compiled exclusively in the USA. All components of the hardware go through a formal incoming inspection and testing process. Final hardware configuration control and quality assurance is performed at our headquarters in Omaha, Nebraska.</p>
<p>12</p>	<p>Describe the extent to which your organization’s suppliers, third-party providers, and customers are included in incident response planning and testing processes, or exercises conducted on a routine and periodic basis.</p>	<p>ES&amp;S has a mature and tested incident response process involving customers, suppliers, DHS and the FBI. ES&amp;S conducts tabletop exercises annually with our customers, state and local law enforcement, DHS, suppliers, and third-party entities to test our incident response plans, and we participate in both customer led and national DHS-led tabletop exercises to test our incident response plans. We use these exercises to gather and analyze lessons learned and integrate new or revised best practices into our plans. In 2018, 2019, 2020 and 2022 ES&amp;S hosted an incident response exercise facilitated by the National Cyber Exercise and Planning Program (NCEPP) National Cybersecurity and Communications Integration Center (NCCIC) U.S. Department of Homeland Security to test our response to multiple major election day incidents. During this engaging, participatory event we walked through scenarios that could involve any part of our organization expected to respond to such an event, and involve our external partners including DHS, the FBI, the ISAC's, our external counsel, our insurer and others to ensure we address the issue(s) and maintain our customer and voter confidence. This event has become an annual one, and we also participate in incident response exercises hosted by others to ensure we are ready to support our customers in any capacity.</p>

## PROTECT

13	<p>Describe how application accounts are requested, created, and maintained to ensure the appropriate data and system access permission levels for job duties are enforced. Also include information on how accounts are monitored for inappropriate activities, suspended when inactive, and removed when personnel change roles or employment is terminated.</p>	<p>New user accounts are generated during the new employee onboarding process when a manager completes a new account request that details the new employee's duties and requested level of network access. This request is reviewed by the IT security staff and approved by HR prior to account creation, ensuring that the principle of least privilege is followed. Requests for escalated privileges are reviewed by the employee's manager and the IT security staff to ensure requested access matches the employee duties. User accounts with elevated privileges are reviewed periodically for continued access requirements. ES&amp;S uses active directory tools to suspend inactive accounts and our HR department issues notices for employees transferring within or separating from ES&amp;S so account privileges can be adjusted accordingly.</p>
14	<p>Describe how your organization facilitates remote access to its own IT systems, and whether multi-factor authentication is required for access at any level.</p>	<p>ES&amp;S enforces the use of a corporate VPN using the Cisco AnyConnect client. All users must use named account network credentials and Duo two factor authentication to connect. We use active directory security groups to limit who has VPN access, and we further segregate what network resources can be accessed by VPN users. The Duo two factor authentication solution also applies to users with elevated privileges and all high profile users.</p>
15	<p>Describe how your organization facilitates remote access to support client systems or devices, and whether multi-factor authentication is used to protect access.</p>	<p>No ES&amp;S tabulation or election management system is configured with remote access software. ES&amp;S has customers who request remote support for other services like ballot definition, ballot creation and general equipment tech support. In those cases we rely upon the customer to initiate a Teams, Zoom or Webex session using the customer managed solution.</p>



<p>16</p>	<p>Describe how your organization tracks and approves authorization and permissions for access to its own IT systems and information. Include all levels of categorization/classification to ensure that personnel, systems, and applications only have access as approved and are limited to the least access that is needed to fulfill the job functions.</p>	<p>Similar to how user accounts are created, user access to network resources is established by active directory security groups and network resources have access control lists that limit access. New user accounts are generated during the new employee onboarding process when a manager completes a new account request that details the new employee's duties and requested level of network access. This request is reviewed by the IT security staff and approved by HR prior to account creation, ensuring that the principle of least privilege is followed. Requests for escalated privileges are reviewed by the employee's manager and the IT security staff to ensure requested access matches the employee duties. User accounts with elevated privileges are reviewed periodically for continued access requirements. ES&amp;S uses active directory tools to suspend inactive accounts and our HR department issues notices for employees transferring within or separating from ES&amp;S so account privileges can be adjusted accordingly.</p>
<p>17</p>	<p>Describe how your organization limits access to network ports, protocols, and services on network devices, and how it utilizes segmentation to minimize vulnerabilities between systems/networks.</p>	<p>ES&amp;S is a Cisco network and has port security features enabled on all corporate IT environment core and edge switches. Only those ports and protocols necessary for validated business functions are enabled. Only authorized devices are allowed to connect to the network. Rogue devices that attempt to connect to the network are rejected and an alert is sent to IT. ES&amp;S ensures that no default configurations or system accesses are present in servers, switches or other devices being introduced to the network. We use customized configurations and access control lists to ensure that network devices can only communicate with other authorized devices. We enforce the "Deny All - Allow by Exception" rules on our network devices, ports and protocols. We manage changes to network device configurations through the use of our IT ticketing</p>

		<p>system, and all network changes are reviewed before being implemented. Our network is micro-segmented, meaning production networks are logically separated from the Test, QA and Development networks and each requires unique user access controls.</p>
18	<p>Describe any access that is provided using a shared account ID accessible to more than one individual user.</p>	<p>ES&amp;S does not allow shared accounts on any network, service or environment. All users are required to utilize named accounts and long, strong passwords as well as Duo two factor authentication. There are no shared accounts in use.</p>
19	<p>Describe how personally identifiable information (PII) and/or information that is deemed confidential or regulated is encrypted when at rest.</p>	<p>The presence of PII and other sensitive information on our network is limited by policy. When PII or sensitive information must be used to support a business process or customer request, this data is encrypted using FIPS 140 standard 256-bit encryption at the file and server level. ES&amp;S encrypts sensitive data at rest at the server and file level using AES 256 encryption controls. All backup files utilize the same AES encryption for data at rest.</p>
20	<p>Describe how personally identifiable information (PII) or information that is deemed confidential or regulated is encrypted when transmitted.</p>	<p>ES&amp;S encrypts sensitive data in motion at the server and file level using AES 256 encryption controls. ES&amp;S utilizes both AES 256 and TLS 1.2 encryption protocols on all internal and external connections where sensitive information is being transmitted. For transfer of data between organizations, ES&amp;S leverages Secure File Transfer Protocol (SFTP) that is closely managed and monitored by our IT Service Center. SFTP ensures data is transferred in an encrypted form and ensures data separation. In instances where it is preferred not to transfer data via a SFTP, ES&amp;S has the ability to leverage encrypted, locking drives capable of storing/transferring large amounts of data. Passwords are provided through secure means to enable decryption and</p>



		unlocking of the secure drive by approved personnel.
21	Describe how data loss and leaks of information are prevented or detected.	<p>S&amp;S uses data segregation and classification, employee education and awareness programs, coupled with a robust data governance policy and network monitoring tools to insure the integrity of our data.</p> <p>ES&amp;S utilizes a data loss prevention tool called Veronis to continuously monitor the corporate network for data leaks or loss. This tool monitors the network for data access and transfers and normal user behavior and alerts the IT staff when abnormal behavior is detected including unusual file transfers.</p> <p>All ES&amp;S employees/contractors enter non-disclosure agreements with ES&amp;S to protect the confidential information of ES&amp;S and its customers. In addition, only those employees/contractors who are assigned to the customer's project or who otherwise have a need to know the customer's information to assist in the completion of the project will be allowed access to the customer's information. ES&amp;S limits access to certain information by restricting files and folders on its system to only those employees/contractors who need to have access to perform the project.</p>
22	Describe how data and devices are protected, including how tamper-evident protections are used to ensure the integrity of software and hardware during shipment and transport to customer locations when supplied by the organization.	<p>ES&amp;S utilizes a central ticketing system and end-to-end chain of custody processes and procedures to ensure that every piece of hardware or software that is delivered to a customer site has full visibility and accountability. We only use certified, bonded delivery services like UPS and Fedex for small shipments. We seal shipments of magnetic media with tamper evident tape. We use our own trucks and delivery employees to deliver hardware. All hardware and software shipments are inspected and signed for at both origination and delivery. We provide complete hardware and software bill of materials (BOM) to</p>

		<p>customers to ensure the integrity of shipments. Every shipment is signed for only by authorized customer representatives.</p>
<p>23</p>	<p>Describe the process used for implementation and ongoing maintenance to prevent, detect, and correct security weaknesses in developed and acquired systems.</p>	<p>Hardening of systems is the process of configuring servers, workstations, and network equipment in an effort to minimize security vulnerabilities and have a standard configuration of the system for each release. Configuration settings are based on security best practices and recommendations from Federal and Industry Standards that provide specific and actionable ways to prevent malicious activity and improve the collective security of the systems, and to achieve acceptable levels of integrity and reliability of voting systems.</p> <p>When an ES&amp;S system or network is hardened, the cybersecurity posture of the network is improved which lowers the risk to outside threats. System hardening also means the systems and network are configured to include only the services, applications, utilities, and settings required to successfully operate the system. By utilizing certified scripts and updates, a standard configuration that has been developed, tested, and certified ensures a secure and reliable voting infrastructure. Moreover, hardening provides many benefits to an system including Security, Reliability, and Standardization. Some elements of this process include:</p> <p>Protect the system from intentional manipulation, fraud, and malicious mischief          Identify fraudulent or erroneous changes to the system</p> <p>Access and functionality is restricted to only that required to operate the systems. Examples of system hardening activities include:</p> <ul style="list-style-type: none"> <li>• Modifying the Windows registry</li> <li>• Configure Account and Local Policies</li> <li>• Configure Software restriction policies</li> </ul>



		<ul style="list-style-type: none"> <li>• Removes non-essential Windows components</li> <li>• Sets permissions on application folders</li> <li>• Configures group-based security permissions</li> <li>• Creates standard configuration of Windows network</li> </ul>
24	<p>Describe how information is backed up, stored and retained, and tested periodically for restoration and recovery.</p>	<p>All servers and critical business files are backed up incrementally every day. A complete recovery backup is made every week. All backups are stored offsite in a secure location. Backups are performed through the use of Commvault to provide the offsite backup at the co-located datacenter operated by TierPoint LaVista. The offsite data centers are far enough away from the corporate offices to minimize the probability that one catastrophe could destroy both primary and backup data. Backups are tested periodically by restoring them to production servers.</p>
25	<p>Describe the physical security characteristics and access control measures of data center environments and facilities associated with data processing for the organization.</p>	<p>ES&amp;S enforces strict physical security precautions at all of its facilities/manufacturing locations to guard both ES&amp;S and customer confidential, proprietary, and trade secrets that could jeopardize the integrity of our production, manufacturing, and development facilities. Examples of these physical controls include: identification badges required for access to all areas, locks and keys to critical information areas, visitor logs/controls within working areas, access limits to sensitive data and computer drives, security guards, security fencing, cameras/motion detectors for controlled areas of the company and our manufacturing facilities, and strict password control for PC and server components of the system.</p> <p>The building where our HQ and primary datacenter is located is covered by 42 continuously operating security cameras, proximity card and user access control and strict visitor escort policies. There is a man-trap style</p>

		<p>             cage at the entrance that authorized users must badge into and then use a combination key lock to enter further into the interior of the datacenter. Only authorized IT staff are on the datacenter access list. There is also fully monitored and redundant HVAC and power to the datacenter.         </p> <p>             ES&amp;S partners with TierPoint for high security co-located datacenter services. TierPoint facilities are state of the art in terms of physical security, utilizing the following controls:         </p> <ul style="list-style-type: none"> <li>• 24x7 security force</li> <li>• continuous internal and external security camera monitoring</li> <li>• electronic door badge readers</li> <li>• bio-metric access controls</li> <li>• strict visitor escort policy</li> <li>• segregation of customer suites and floorspace</li> <li>• intrusion detection and alarm systems</li> <li>• fully monitored and redundant HVAC and power</li> </ul> <p>             TierPoint undergoes a variety of assessments of all its datacenters annually including PCI-DSS, SOC 2, HIPAA, NIST 800-53, LEED, Gramm Leach Bliley, and NERC.         </p>
<p>26</p>	<p>Describe the organization’s availability, uptime, and failover processes and standard measures of performance.</p>	<p>             ES&amp;S strives to achieve maximum system availability and uptime that align with industry standards and best practices. Our primary and DR datacenter managed by TierPoint are n+2 configurations meaning there are multiple facility power, HVAC and circuit paths to ensure maximum up time. While we do not perform full system failover tests, we do test our emergency generator weekly, and we utilize rigorous change control processes to minimize system outages due to planned maintenance, and we triage any unplanned outage to ensure any deviation from change control processes are addressed.         </p>



27

Describe the vetting process your organization uses during the personnel selection and onboarding process, as well as any periodic ongoing checks of personnel backgrounds.

ES&S conducts background checks on all employees (full-time and temporary) and contractors prior to commencement of work for our company. A successful background check must include:

- No felony convictions
- No outstanding bench warrants or outstanding arrest warrants
- No misdemeanor convictions within the previous five years for a crime involving violent behavior, vehicular homicide, some element of deceitfulness, untruthfulness, or falsification bearing on the new hire's propensity to be truthful and honest, including but not limited to, crimes such as theft, burglary, and check fraud.
- No more than one misdemeanor conviction within the previous five years for a crime involving driving under the influence or reckless/aggressive driving. This finding will apply only to those positions that require the candidate to operate a company-owned or rented vehicle or heavy machinery, or where ground travel is a significant component of the applicable position.

ES&S employees undergo fingerprint checks on an as-needed basis, depending on client requirements.

All Associates are required to wear an assigned Identification Badge daily while on ES&S' worksites. Associates representing ES&S off-site may also be required to wear their ID badge off ES&S premises. Failure to regularly display the assigned badge, frequent loss of badges, or unauthorized loan of an ID badge to another individual is a violation of ES&S policy and could result in disciplinary action, up to and including termination.

As employees of ES&S, Associates accepted an obligation to help ES&S preserve and protect its confidential and proprietary information. ES&S confidential and proprietary information includes, but is not limited to, customer lists,

product plans, new material research pricing lists, marketing plans, customer files, proposals, certification documentation, employee information (including medical), contracts, vendor agreements, production processes and budgets.

The following are examples of how Associates protect ES&S' confidential, proprietary information:

Monitor their work area for sensitive information and do not leave proprietary and confidential information unattended. to source code, designs, financial information, Remain alert in common meeting areas. Monitor their office and telephone conversations.

Be responsible for their computer system and equipment (includes printers, copiers, and faxes). Ensure understanding of the ES&S network. Protect file cabinets, desk drawers, and storage items. Share only appropriate information with vendors, consultants, and personal acquaintances.

At ES&S, Associates must respect ES&S' confidential information and knowingly share necessary information only with appropriate parties. Failure to abide by this policy may result in disciplinary action, up to and including termination. ES&S understands the current cybersecurity environment, as well as the focus and concern surrounding election security. ES&S is making continuous investments to bolster our security systems and processes, strengthen our depth of defenses, and identify and resolve vulnerabilities. ES&S will continue to maintain our obligation of securing and protecting the interests of our customers and of voters as our most critical priority. For example: Candidates that do not pass a background check are not hired. ES&S does not perform annual



		<p>background checks but reserves the right to perform additional checks if required.</p>
<p>28</p>	<p>Describe how your organization conducts security awareness training for the organization as well as specific training for roles associated with privileged users.</p>	<p>ES&amp;S requires all contractors, subcontractors, vendors, outsourcing ventures, or other external third- parties to comply with ES&amp;S security policies and customer agreements. We ensure this compliance by conducting periodic reviews of third-party performance and contract reviews. We carefully monitor any third-party access to network resources and utilize the concept of least privilege to ensure these entities only have the access needed to perform their functions.</p> <p>ES&amp;S employs a comprehensive security awareness program, staffed by a corporate security awareness team. ES&amp;S has a comprehensive security plan and training program that all employees, contractors, temps and interns (ECTi) are required to follow as a condition of employment.</p> <p>Security indoctrination and awareness training starts during the first week of onboarding when each new ECTi meets with ES&amp;S' Vice President of Security where he provides a 1-hour briefing on the ES&amp;S security awareness and training plan. Within 7 days of onboarding each ECTi receives an email from the training department inviting them to complete a comprehensive computer-based security awareness training program. This training program, procured from KnowBe4 and updated frequently, covers a wide range of cyber and physical security threats, mitigating controls, realistic scenarios, and content module quizzes that the trainee must pass successfully to obtain continued access to company network resources. This training program emphasizes good cyber hygiene to be used at home and at work to build a respect for and awareness of cyber threats to our business. The completion date of this initial training becomes the anniversary date and basis for our</p>

		<p>training department to track completion of the training on an annual basis thereafter. ES&amp;S also utilizes the KnowBe4 enterprise phishing training tool and all employees, contractors, temps and interns are automatically enrolled and phished by the automated program at least once every three months. Users who fail the phishing exercise are provided immediate feedback on what they did wrong. Users who fail the phishing exercise more than once receive additional remedial training designed to increase awareness of the phishing threat and the consequences of continued risky behavior. Finally, the VP of Security, supported by the corporate security awareness team, HR and Marketing departments communicate cybersecurity awareness of issues and best practices through regular (monthly and bi-weekly) communications campaigns using email, workplace posters and bulletins. ES&amp;S also conducts quarterly informational “security lunch-and-learns” where ECTi’s receive timely, interactive information on security.</p>
<p>29</p>	<p>Describe your organization’s policy on collection, retention, and review of audit/event log records.</p>	<p>ES&amp;S collects system and security logs from all network components and utilizes Splunk scripts to look for anomalies in normal system behavior and other indicators of compromise. ES&amp;S provides our logs to a third-party managed security service company for additional review. ES&amp;S maintains log files for 90 days.</p>
<p>30</p>	<p>Describe the processes used to define, implement, and maintain standard configurations and hardened configuration settings for your organization’s technology systems.</p>	<p>ES&amp;S configures every network appliance and end user device with the approved corporate IT configuration and security controls before delivery or attachment to the network. There are no default account user names or passwords allowed. ES&amp;S uses a gold disk image to create standard network endpoint software deployments. This image contains licensed versions of all commercial software that our workforce requires to conduct business. Users who desire</p>



		<p>additional software must initiate a service request ticket to the IT service center and once approved will then add authorized software to the user device.</p> <p>We are a VMware shop so we create and deploy our own server images across all of the production, test, QA and development server environments. ES&amp;S ensures that no default configurations or system accesses are present in servers, switches or other devices being introduced to the network. We use customized configurations and access control lists to ensure that network devices can only communicate with other authorized devices. We enforce the "Deny All - Allow by Exception" rules on our network devices, ports and protocols. We manage changes to network device configurations through the use of our IT ticketing system, and all network changes are reviewed before being implemented. Our network is micro-segmented, meaning production networks are logically separated from the Test, QA and Development networks and each requires unique user access controls.</p>
<p>31</p>	<p>Describe the protections your organization deploys to reduce the attack surface exposed to end users through email, internet websites, and social media.</p>	<p>In addition to our comprehensive security awareness training program and internal phishing programs, ES&amp;S employees are prohibited from sharing any sensitive company or customer information by our confidentiality and nondisclosure agreement that is signed on the first day of employment and reviewed annually thereafter.</p> <p>The use of personal email and any social media for company business is prohibited. The ES&amp;S public-facing internet website <a href="http://www.essvote.com">www.essvote.com</a> is hosted by a third-party web hosting company in another state and has no physical or logical connection to the ES&amp;S corporate IT or production network.</p> <p>ES&amp;S enforces an acceptable use policy with all users that defines what is allowed on corporate</p>

		<p>devices and networks, as well as what is prohibited. ES&amp;S uses embedded Microsoft O365 email filters and security controls, as well as Mimecast Email security filters for the prevention of malicious email, attachments and links. ES&amp;S uses Cisco Talon and other tools for reputation-based blocking of malicious websites. The ES&amp;S Marketing and Public Affairs team monitors employee social media footprints for compliance with company policy.</p>
<p>32</p>	<p>Describe the protections your organization uses to secure and prevent unauthorized access to Wi-Fi networks.</p>	<p>ES&amp;S maintains separate employee and guest wireless networks. The ES&amp;S corporate Wi-Fi is only accessed by named users using authorized network credentials and two factor authentication. The guess Wi-Fi access must be arranged through the IT team. There is no open Wi-Fi access.</p> <p>Employees desiring access to the corporate wireless network must submit a request to the IT Service Desk identifying the device to be used and the business case for access. The IT security team reviews the request and if approved grants access to the corporate wireless by adding the device MAC address to the access control list. Guests requesting access to the guest wireless must submit the request through their employee sponsor. Again, IT reviews the request and if approved gathers the MAC address of the guest device and adds it to the guest wireless AC, then issues the guest a temporary username and password. They guest wireless network is severely restricted to only provide internet access.</p>
<p><b>DETECT</b></p>		
<p>33</p>	<p>Describe the process your organization uses to monitor events and analyze cybersecurity threats, attacks and suspicious activity.</p>	<p>ES&amp;S uses a variety of automated security tools, rules and controls to prevent unauthorized access to the infrastructure and customer information. In addition to using 2 different AV/Malware detection and prevention systems on all endpoints, ES&amp;S utilizes DHS to conduct</p>



		<p>cyber hygiene scans of our public facing systems weekly.</p> <p>ES&amp;S collects system and security logs from all network components and utilizes Splunk scripts to look for anomalies in normal system behavior and other indicators of compromise. ES&amp;S provides our logs to a third-party managed security service company for additional review. ES&amp;S has installed 5 Albert sensors in our hosted voter registration environment which look for indicators of compromise.</p> <p>ES&amp;S has also installed Veronis, a network-based data loss detection and prevention application which alerts system administrators and security personnel to unusual user behavior and unauthorized access requests. ES&amp;S maintains log files for 90 days.</p>
<p>34</p>	<p>Describe how your organization prevents the installation, spread, and execution of malicious code and utilizes layers of defense to maximize automation to enable rapid updating of protections against quickly evolving malicious code.</p>	<p>The ES&amp;S IT team monitors all the vendors whose equipment and software we use and applies any needed patches after testing and in accordance with the CVSS rating and timeline described above. ES&amp;S has also deployed both Sophos and the Cisco AMP for Endpoints suite of products across all laptops and desktops which provides maximum protection against the most advanced attacks. It prevents breaches and blocks malware at the point of entry by quarantining the infected device, then rapidly detects, contains, and remediates advanced threats that evade front-line defenses. We do not allow BYOB or personal devices on the corporate network or in any production or development environment. ES&amp;S uses Microsoft WSUS which is a program developed by Microsoft to manage hotfixes and updates to Windows environments.</p>
<p><b>RESPOND</b></p>		
<p>35</p>	<p>Describe how your organization implements incident response plans</p>	<p>ES&amp;S has a mature and tested incident response process involving customers, suppliers, DHS and the FBI. ES&amp;S follows the 2018 Department of</p>



<p>as well as how it manages incidents as they are detected and responded to. Include how your organization uses lessons learned and proactive reviewing and testing to continually improve processes and protection capabilities.</p>	<p>Homeland Security publication titled: Incident Handling Overview for Election Officials that instructs election entities on how to inform DHS about cyber-related incidents.</p> <p>Our incident response policy and processes are used to analyze potential cyber incidents and triaged by our internal team of subject matter experts, and where circumstances indicate, the reporting of the incident to government officials we follow DHS guidelines for alerting the NCCIC, MS-ISAC and EI-ISAC.</p> <p>In the unlikely event of a security incident, ES&amp;S works closely with affected customers to identify and mitigate the incident to restore voting, tabulation and reporting functions as soon as possible. We employ an eight-step incident response plan including 1.) initial triage; 2.) communications with customers; 3.) engagement with vendor partners and law enforcement; 4.) full incident triage; 5.) incident containment; 6.) incident eradication; 7.) system recovery; and 8.) restoration of services.</p> <p>ES&amp;S conducts tabletop exercises annually with our customers, state and local law enforcement, DHS, suppliers, and third-party entities to test our incident response plans, and we participate in both customer led and national DHS-led tabletop exercises to test our incident response plans. We use these exercises to gather and analyze lessons learned and integrate new or revised best practices into our plans.</p>
--	---

**RECOVER**

<p>36 Describe your organization’s implementation of the continuity of operations plan and how this plan is managed once activated.</p>	<p>ES&amp;S has a business continuity and disaster recovery plan that dictates how systems and data are protected in the event of a disruption in operations. Our plan identifies all ES&amp;S facilities, mission critical systems, individuals responsible for executing the plan, and recovery time objectives that support ES&amp;S and customer requirements.</p>
---	--

	<p>Each location that holds, stores or retains data must follow the corporate BC/DR that includes backup and recovery procedures for all data, software applications, email and phone systems. In a situation in which facilities are damaged and cannot be used, a warehouse, hotel suite or rental office space with internet connectivity can be used as a temporary base of operations. For the first 24 to 72 hours following a disaster, we will rely on redundant capabilities at other sites where possible to maintain our operations. Following that, personnel at the disaster location will be able to resume operation at a temporary location. Finally, regular operations will be restored at a permanent location.</p> <p>ES&amp;S has established a DR working space at a site 3 miles from our HQ that allows for the relocation of mission critical personnel and equipment. All connectivity necessary to continue operations is available at this site and we have tested it prior to the 2020 and 2022 general election.</p> <p>All servers and critical business files are backed up incrementally every day. A complete recovery backup is made every week. All backups are stored offsite in a secure location. Backups are performed through the use of Commvault to provide the offsite backup at the co-located datacenter operated by TierPoint LaVista. The offsite data centers are far enough away from the corporate offices to minimize the probability that one catastrophe could destroy both primary and backup data.</p>
--	--

VERIZON WIRELESS – Vendor Risk Management Policy

IDENTIFY		
1	Describe how your organization actively tracks and manages authorized hardware devices and systems to	Assets are tracked and inventoried in one of the Verizon-approved central repositories using the Verizon Information Resource name and documenting associated asset details.

## POLICY

	ensure that unauthorized devices and systems are identified and prevented from gaining access.	Access controls protect from unauthorized access to any of Verizon's environments.
2	Describe how your organization actively tracks and manages authorized software to ensure that unauthorized software and applications are identified and prevented from installation or execution.	Users' abilities are restricted from installing unapproved documented applications, and instituting blacklisting and whitelisting techniques to prevent unauthorized software from being installed.
3	Describe how your organization tracks and manages authorized data flows, application programming interfaces (APIs), and the extraction of data to ensure unauthorized access and removal of data does not occur.	Data is managed in a systematic, structured manner to enforce confidentiality, integrity and availability requirements. Data protection policies combined with data loss prevention processes, procedures, and tools are designed to reduce risk of exploitation, alteration or unauthorized disclosure.
4	Describe how information resources are classified and categorized to ensure appropriate controls for protection and timely recovery, as well as for retention and planned destruction.	Verizon and its affiliates' data are classified (i.e., Public, Private, Confidential, and Highly Confidential information) taking into account its value to the organization and the potential business impact from its loss or change.
5	Describe how your organization ensures that personnel have the required expertise and skills to perform their job duties and how they are trained on an ongoing basis to maintain required skills.	Supplemental, role-based training is provided to all personnel. Employee managers routinely assess performance and provide coaching and feedback, as applicable.
6	Describe your organization's processes for identifying vulnerabilities within the information technology environment and network infrastructure and how remediation is performed to minimize exposure to threats and attackers.	Procedures to manage vulnerabilities (e.g., scanning, patching, remediating, mitigating and deploying compensating controls) are documented and followed. A vulnerability management program ensures that Verizon has sufficient scanning tools, penetration testing, anti-virus coverage, and patch management procedures to decrease the risk of vulnerabilities in the business environment.
7	Describe how your organization tests the overall strength of defenses and simulates the actions of attackers, including penetration tests that are conducted periodically.	Detection roles and responsibilities are clearly defined and assigned to personnel performing security scanning or penetration testing, conducting vulnerability assessments, monitoring event logs, assessing industry/vendor vulnerability trends, etc. on a routine basis.
8	Describe how your organization assesses, addresses, and accepts cybersecurity risks.	The Verizon CyberSecurity organization is responsible for providing compliance guidance as detailed in the underlying standards and control framework. Deviations from controls that satisfy policy statements require a consultation with the Verizon Business Unit Information Security Organization and an exception or risk acceptance approval from business unit leadership.
9	Describe your organization's processes for managing the development, testing, and quality assurance of applications, software, and client configurations to ensure vulnerabilities within your products are identified and remediated.	Detection processes are configured in compliance with security standards, regulations, and control framework, and tested at regular intervals for performance, compliance, and flexibility to detect evolving threats as well as remediating vulnerability. Testing detection processes ensure that they remain compliant with relevant regulations, minimize false-positive findings, and are able to detect new threats, vulnerabilities or events.
10	Describe the methodology and sources your organization uses to monitor the threat landscape and	Internal and external threat information feeds are used to monitor and stay abreast of threats and vulnerabilities. All



	<p>obtain cybersecurity threat intelligence and indicate if your organization participates as a member of the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC).</p>	<p>identified applicable threats are documented in a risk register. Verizon publishes cybersecurity threat intelligence via the Data Breach Investigations Report (DBIR) that addresses all elements of risk, not only cyber criminals or nation-state threat actors, but human negligence, misuse or simple error. Verizon participates as a member with the EI-ISAC organization.</p>
11	<p>Describe the assurance process your organization uses to evaluate cybersecurity risks and the capabilities within your organization's supply chain and supplier environment to mitigate them.</p>	<p>Daily business operations involve both onsite and remote interactions with suppliers, vendors, managed service providers, contractors and other third parties. Risk is minimized before engaging with third party partners by assessing third party access to sensitive assets, performing due diligence to evaluate any lapses in third party security, and including appropriate liability language in formal agreements and contracts. During their engagement, third parties are monitored and included in response and recovery planning to ensure accountability for maintaining an acceptable level of security and for supporting response and recovery efforts when they are liable.</p>
12	<p>Describe the extent to which your organization's suppliers, third-party providers, and customers are included in incident response planning and testing processes, or exercises conducted on a routine and periodic basis.</p>	<p>Verizon's corporate Incident Response Plans, and changes to the plans, are distributed to defined stakeholders and organizations at least annually. For custom managed solutions where customer's have specific incident response requirements and deliverables, Verizon will include the customer in the planning and response process and factor any custom deliverables into the proposed solution to the customer.</p>
<b>PROTECT</b>		
13	<p>Describe how application accounts are requested, created, and maintained to ensure the appropriate data and system access permission levels for job duties are enforced. Also include information on how accounts are monitored for inappropriate activities, suspended when inactive, and removed when personnel change roles or employment is terminated.</p>	<p>Access credentials uniquely identify an individual person, system or service, and are adequately safeguarded. Proper business approval is documented prior to an individual account creation or access provisioning and are granted as required to perform their specified job function. Access is reviewed on a periodic basis to validate that it is still required. Security Continuous Monitoring (logging) performs real-time analysis and assessment on Verizon's information systems and assets and user accounts that looks for policy violations. All access is de-provisioned or removed as it is no longer required or in the event of a termination.</p>
14	<p>Describe how your organization facilitates remote access to its own IT systems, and whether multi-factor authentication is required for access at any level.</p>	<p>All remote network connections to systems and networks, such as remote desktop, and remote assistance, are individually identified, verified, logged, and reviewed by the Verizon CyberSecurity organization and approved by the business. Authentication mechanisms (e.g., MFA, passwords, pass-phrases, tokens, biometrics, user behavior) are strongly constructed and used in a manner that prevents unauthorized access.</p>
15	<p>Describe how your organization facilitates remote access to support client systems or devices, and whether multi-factor authentication is used to protect access.</p>	<p>All remote network connections to systems and networks, such as remote desktop, and remote assistance, are individually identified, verified, logged, and reviewed by the Verizon CyberSecurity organization and approved by the business.</p>

## POLICY

		Authentication mechanisms (e.g., MFA, passwords, pass-phrases, tokens, biometrics, user behavior) are strongly constructed and used in a manner that prevents unauthorized access.
16	Describe how your organization facilitates remote access to support client systems or devices, and whether multi-factor authentication is used to protect access.	Access credentials uniquely identify an individual person, system or service, and the access credentials are adequately safeguarded. Verizon and its affiliates' data are classified (i.e., Public, Private, Confidential, and Highly Confidential information) taking into account its value to the organization and the potential business impact from its loss or change. User access is based on an individual's systems or process function and follow the principle of least privilege, where the minimum access levels granted provide the least amount of access required to perform their function and the sensitivity of the information they are trying to access.
17	Describe how your organization limits access to network ports, protocols, and services on network devices, and how it utilizes segmentation to minimize vulnerabilities between systems/networks.	Access controls use security mechanisms to enforce defined access permissions to specific individuals, systems or processes, in both the digital and physical environments. The controls reduce the risk of accidental or deliberate modification, destruction, or dissemination of information, as well as protect from unauthorized access to any of Verizon's environments (e.g., physical locations, internal Information Technology (IT), or shared public cloud).
18	Describe any access that is provided using a shared account ID accessible to more than one individual user.	The use of shared interactive IDs should be minimal, assigned to a Verizon responsible party, have very limited capability, and approved through an auditable approval process. Additional technical controls and manual processes should be implemented to validate that shared account activity is approved, used by authorized individuals and traced back to users for accountability.
19	Describe how personally identifiable information (PII) and/or information that is deemed confidential or regulated is encrypted when at rest.	Verizon policy requires that VZ highly confidential data elements are encrypted at rest.
20	Describe how personally identifiable information (PII) or information that is deemed confidential or regulated is encrypted when transmitted.	Protecting data throughout its life cycle enables the availability of critical information when required, preserves the integrity of critical data in-transit and at-rest and protects sensitive information from unauthorized access or disclosure. Verizon uses multiple encryption approaches to protect PII including, but not limited to, file/folder-level, full disk, hardware, e-mail, chat, other messaging technologies, database/file, etc. dependent on the product/service.
21	Describe how data loss and leaks of information are prevented or detected.	Data Loss Prevention (DLP) a set of procedures and mechanisms to stop sensitive data from leaving a security boundary. Technologies may perform: 1. Content inspection; 2. Contextual analysis of data sent via Instant Messenger (IM) or email; 3. Inspection of data in motion; 4. Inspection of data in use on a managed endpoint device; and 5. Inspection of data at rest (including on premise and cloud.)



## POLICY

22	Describe how data and devices are protected, including how tamper evident protections are used to ensure the integrity of software and hardware during shipment and transport to customer locations when supplied by the organization.	Data is managed in a systematic, structured manner to enforce confidentiality, integrity and availability requirements throughout its lifecycle: creation, use, transmission, storage, modification, retention, and destruction. Equipment shipments are delivered to the customer that leave a Verizon warehouse or a supplier/TPV warehouse across the globe that are securely packaged and sealed. Upon delivery receipt the customer will inspect the box to determine whether the integrity of the box was tampered and the contents suspect. International shipments will follow import/export regulations; special encryption units follow ITAR regulation.
23	Describe the process used for implementation and ongoing maintenance to prevent, detect, and correct security weaknesses in developed and acquired systems.	Asset maintenance, as well as repair services, by authorized personnel are approved and recorded prior to being performed and will be conducted in a timely manner. Service Level Agreements (SLAs) are established for the maintenance of critical assets. Change authorization and logging must use approved tools.
24	Describe how information is backed up, stored and retained, and tested periodically for restoration and recovery.	System Maintenance may include: 1. On-site maintenance; 2. Off-site maintenance or equipment repair; and 3. Use of remote maintenance and diagnostic tools and connections. Formal change control procedures are documented and enforced to ensure the integrity of system, applications and products, from the early design stages through all subsequent maintenance efforts. Backup copies of data and software information are collected at regular, planned intervals, stored in a secure location, protected according to the classification of the data contained, and tested periodically to verify the backup, data integrity and restoration processes are operating correctly, as applicable.
25	Describe the physical security characteristics and access control measures of data center environments and facilities associated with data processing for the organization.	All critical facilities (including data centers, networks, telecommunication equipment, sensitive physical material and other important assets) are physically protected against accident or attack and unauthorized physical access. Physical access to buildings and critical infrastructure (e.g. computing facilities, network infrastructure) are restricted to authorized personnel with a legitimate business need. Physical access controls are necessary to protect against theft, business interruption and unauthorized access.
26	Describe the organization's availability, uptime, and failover processes and standard measures of performance.	Dependent on the product/service, as applicable, corresponding Service Level Agreements (SLAs) will contractually define role and responsibilities of the service provider, customer, and layout performance benchmarks and reporting for the product/service being ordered.

## POLICY

27	Describe the vetting process your organization uses during the personnel selection and onboarding process, as well as any periodic ongoing checks of personnel backgrounds.	<p>Verizon's onboarding standards will perform a background investigation that includes: 1. Confirmation of academic and professional qualifications; 2. Investigation of any loss of professional credentials; 3. An identification check (e.g., to include verification of past three (3) employments, court records and all places of residence and employment for the past seven (7) years); 4. A check of county, state, federal, national and international (where permissible) police records for criminal history for at least the past seven (7) years; 5. A drug test; 6. OFAC screening; 7. Sex offender registration status; 8. Confirmation of identity from government-issued identification; and 9. For personnel not residing within the U.S. for at least seven years prior to the date of the check, background checking consistent with industry best practice for the jurisdiction. Verizon management follows Human Resources onboarding checklists that defines a standard interviewing process for personnel selection. Examples of onboarding may include: 1. Acknowledgement of Code-of-Conduct which includes information security responsibilities; 2. Sign-off on non-disclosure agreements: a. An employee may be required to sign an additional non-disclosure or confidentiality agreement prior to accessing Verizon non-public information; b. A non-disclosure agreement or applicable third party contract covers access to Verizon non-public information by contract staff, contractors, vendors or other third parties; 3. Appropriate role assignment to ensure separation of sensitive duties; and 4. Completion of Information Security Awareness and Training.</p>
28	Describe how your organization conducts security awareness training for the organization as well as specific training for roles associated with privileged users.	<p>Verizon's security awareness program promotes and embeds expected security behavior in all employees and contractors who have access to Verizon's information, systems, and network assets and reduces the risk of insider threats caused by malicious behavior, negligent behavior, and accidental behavior of Verizon personnel.</p>
29	Describe your organization's policy on collection, retention, and review of audit/event log records.	<p>Important events (e.g., application, system, network or data access, configuration changes, failures or privileged activity) with potential security implications are defined and recorded in logs. Logs help identify threats that may lead to an information security incident, maintain the integrity of important security-related information and support forensic investigations. Retain security event log data per legal and regulatory requirements.</p>
30	Describe the processes used to define, implement, and maintain standard configurations and hardened configuration settings for your organization's technology systems.	<p>A secure baseline configuration incorporating security principles (e.g., concept of least functionality) is designed and maintained for systems and technical infrastructure protecting sensitive information and used in all new deployments. Verizon's CyberSecurity baseline security configuration standards for newly installed, hardened and deployed infrastructure components is developed. This baseline ensures that security controls are deployed consistently across the environment, which in turn will decrease the risk of asset security vulnerabilities.</p>

31	Describe the protections your organization deploys to reduce the attack surface exposed to end users through email, internet websites, and social media.	The Verizon Information Security Organization, pertaining to the access of personal email accounts (i.e., Gmail), internet websites (i.e., content that violates corporate policy), and social media outlets (i.e., Facebook, Twitter) using Verizon Information Resources is strictly prohibited for use on corporate assets as it is construed as an avenue for loss of Verizon data. Verizon secures their network perimeter using defense in depth toolsets, industry standards and best practice, policy enforcement and governance, and training and awareness programs aimed at protecting the organization and its customer base.
32	Describe the protections your organization uses to secure and prevent unauthorized access to Wi-Fi networks.	Verizon has a Wireless Security policy that has been approved by management, communicated to appropriate constituents, and has an owner to maintain and review the policy. Wireless connections are secured with WPA2, and encrypted using AES or CCMP. The policy permits approved and/or vendor supported wireless access points, and prohibits wired and wireless network connections at the same time. The policy requires sensitive Wireless networks to be authenticated using multi-factor authentication, and requires continuous monitoring and alerting to security personnel, or quarterly scanning for rogue wireless access points. All wireless networks require penetration testing at least annually.
<b>DETECT</b>		
33	Describe the process your organization uses to monitor events and analyze cybersecurity threats, attacks and suspicious activity.	Security event data from multiple sources (e.g., logs, network packets, file hashes) are correlated, reviewed and analyzed on a regular basis. The review frequency (periodic - real-time) are in line with the risk associated with the monitored asset. Multiple log sources are correlated to improve detection capabilities. Without constant vigilance, security incidents can go unnoticed, potentially prolonging the incident and increasing the overall impact to the organization.
34	Describe how your organization prevents the installation, spread, and execution of malicious code and utilizes layers of defense to maximize automation to enable rapid updating of protections against quickly evolving malicious code.	Verizon uses defense in depth mechanisms to protect against malicious code. To strengthen boundary protection, managed interfaces including gateways, routers, firewalls, guards, network-based malicious code analysis, virtualization systems, or encrypted tunnels implemented within a security architecture are continually monitored. Segregation of Duties is another internal control that prevents or detects errors and irregularities by assigning two separate individuals the responsibility for initiating and recording transactions, and for the custody of assets where no single person will be in a position to introduce fraudulent or malicious code without detection. Verizon also scans maintenance tool media for malicious code prior to use to validate integrity. Any monitoring and scanning devices are vetted and approved by Information Security before their use to reduce the risk of unintentional impact on the network or introduction of malicious code into the environment. Verizon actively monitors code for malware via monitoring solutions that look for signature based and behavior based code. As security events are generated, security alerts are automatically



distributed to appropriate security personnel for immediate action when defined thresholds are exceeded.

RESPOND

35

Describe how your organization implements incident response plans as well as how it manages incidents as they are detected and responded to. Include how your organization uses lessons learned and proactive reviewing and testing to continually improve processes and protection capabilities.

Verizon's corporate incident response plans outline formal reporting and response procedures that are established, documented, tested, and followed when responding to security incidents. Without a clearly defined incident response plan, it may not be possible to: a) Detect, classify, and alert on potential security events as they appear in the business environment; b) Escalate identified security events to the proper incident response personnel in a timely manner; c) Contain a security incident to minimize its spread across the network and to allow for forensic evidence capture where prudent and practical; and d) Execute response measures to eradicate malware from the environment, get critical systems back online, take appropriate legal action against individuals, and at the direction of the CISO notify internal stakeholders and third parties of breaches. Roles and responsibilities in the incident response plan are defined and clearly articulated so that incident response personnel are aware of and can act upon the order of operations necessary to respond to a security incident. Incidents are categorized by their severity according to event impact indicators and event type descriptions outlined in the Incident Response Plan. Verizon updates its Incident Response Plan to reflect key takeaways learned from previous security incidents, evolving threats, and from mock incidents or incident response testing.

RECOVER

36	Describe your organization's implementation of the continuity of operations plan and how this plan is managed once activated.	Verizon's Business Continuity owner or custodian will perform a technology asset inventory to determine and document the mission-critical technology components, their location, how they're configured, and who is responsible for management. The owner or custodian will determine what measures should be taken to protect and recover these components. The custodian will document the Business Continuity Plan for functions supporting their critical information resources, ensure the Business Continuity Plan is stored in a centralized repository, and will make the Business Continuity Plan accessible to those resources who need to view it. If a system supports one of these five functions (i.e., 1. Voice, Data and Media Services Delivery, E911; 2. Managed Services Delivery; 3. Ordering, Provisioning and Installation; 4. Maintenance and Repair; and 5. Billing and Financial Management) they have a Business Continuity and Disaster Recovery plan. Plans may be product/service specific and may require include the use of an alternate processing and storage site that is geographically separate from the primary site(s). Verizon's business units conduct a Business Impact Analysis (BIA) at the commencement of their Business Continuity and Event Management Program, prior to plan development, and annually on an ongoing basis.
----	---	---





**PANOLA COUNTY 2023 BUDGET JAIL COMMISSARY**  
**November 27, 2023**

ACCOUNT	ACCOUNT DESCRIPTION	AMOUNT	
<b>JAIL COMMISSARY FUND</b>			
<b>REVENUE</b>			
810-360-41155	COMMISSARY PROFITS	<u>2,000</u>	<u>2,000</u>
<b>EXPENDITURES</b>			
810-460-55270	FURNITURE & EQUIPMENT	<u>2,000</u>	<u>2,000</u>
<b>GRAND TOTAL JAIL COMMISSARY</b>			<u>2,000</u>

I hereby approve the above described budget and ask the Commissioners Court to please record it at the next scheduled Commissioners Court Meeting.

\_\_\_\_\_  
Cutter Clinton, Panola County Sheriff

# Sabine River Authority of Texas

## Community Assistance GRANT Program

### Application Form

Each entity must submit a completed **Community Assistance Grant Application form** to be considered for funding. Applications are valid for one-year from date of receipt and are considered for funding quarterly by the Sabine River Authority Board of Directors.

(Please type or print the requested information below)

#### Entity Information

Name of Entity (County/City/District etc.)

Panola County (Sharpe-Field Airport)

Address

110 S. Sycamore, Rm 216-A

County

Panola

City State ZIP Code

Carthage, TX 75633

Contact Person

Rodger McLane, County Judge

FAX No.

(903) 693-2726

Telephone No.

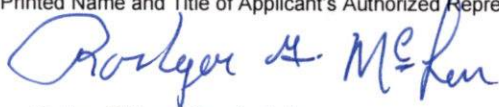
(903) 693-0391

Email Address

Rodger.McLane@co.panola.tx.us

**Project Description** Provide a brief description of the Project. Refer to Grant Application Instructions for details. Additional sheets may be added if needed.

Airport water main extension from Quail Creek Dr to Airport Driveway (see provided estimate).

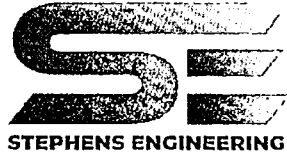
<b>Project Category</b> - costs could include feasibility studies, materials or construction costs for:	<b>Check one Category that best describes the purpose of the Project</b>
<b>A. Water Supply System</b> – Permitted capacity of a Water Supply System is being expanded or additional facilities are needed for growth.	X
<b>B. Wastewater Management</b> – Permitted capacity of a Wastewater Treatment System is being expanded or additional facilities are needed for more stringent limits.	
<b>C. Water Conservation</b> - Promotes or improves water use efficiency.	
<b>D. Water Quality</b> - Promotes or improves instream water quality.	
<b>Requested Amount:</b> (up to \$20,000)	\$ <u>20,000</u>
<b>Local Commitment:</b> (Amount of Local Funds)	\$ <u>158,343</u>
<b>In-Kind Services:</b> (Describe and value)	\$ _____
<b>Other Sources of Funds:</b> (Describe)	\$ _____
<b>Total Project Costs:</b>	\$ <u>178,343</u>
<b>Links to Other State/Federal Loan or Grant Programs:</b> (Identify program and status of approval)	
<b>Signature of Legally Authorized Public Official</b>	
Printed Name and Title of Applicant's Authorized Representative  Rodger McLane, County Judge	Phone Number:  (903) 693-0391
Signature of Authorized Representative	Date:

**Mail**

- 1) Completed application
- 2) Supporting documentation
- 3) Map of project area

**Sabine River Authority of Texas  
Community Assistance Program  
P. O. Box 579  
Orange, TX 77631**

Address questions to:  
**Zach Johnson**  
Phone: 409-746-2192  
Fax: 409-746-3780  
Email: [cap@sratx.org](mailto:cap@sratx.org)



P.O. Box 6618  
Longview, TX 75608

Texas Registered Engineering Firm F-20395

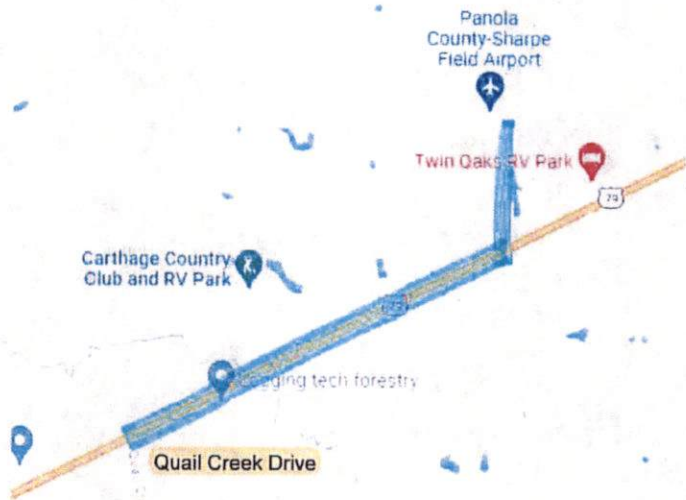
O: 903.215.8990  
stephenseng.net

Panola County  
Airport Water Main Extension  
Opinion of Probable Construction Cost

<u>Description</u>	<u>Qty.</u>	<u>U/M</u>	<u>Unit Cost</u>	<u>Total Cost</u>
<b><u>Quail Creek Dr to Airport Driveway</u></b>				
1 . Furnish and install 6" C900 water main w/locator wire	3470	LF	\$29	\$100,630
2 . Directional bore restrained joint water main	600	LF	\$65	\$39,000
3 . Tie into existing water main w/tapping sleeve and valve	1	EA	\$3,000	\$3,000
4 . Tie into existing 6" water main w/tapping sleeve and valve	1	EA	\$4,000	\$4,000
5 . Furnish and install fire hydrant assembly, complete, in place	2	EA	\$6,000	\$12,000
6 . Furnish and install 2" short side water service	1	EA	\$2,500	\$2,500
7 . Hydrostatic testing and disinfection	1	LS	\$1,000	\$1,000
Subtotal =				\$162,130
Subtotal				\$162,130
Contingencies (10%)				\$16,213
Total Opinion of Probable Construction Cost				\$178,343

# PRELIMINARY

THIS DOCUMENT IS RELEASED FOR THE  
PURPOSE OF INTERIM REVIEW UNDER  
THE AUTHORITY OF KYLE A. STEPHENS,  
P.E. NO 106333 ON 10/4/23 . IT IS NOT  
TO BE USED FOR CONSTRUCTION.



Panola  
County-Sharpe  
Field Airport

Twin Oaks RV Park

Carthage Country  
Club and RV Park

logging tech forestry

Quail Creek Drive

79



# Sabine River Authority of Texas CAP – GRANTS Applicant Eligibility

## ELIGIBLE APPLICANTS<sup>1</sup>:

### Governmental Entities that are:

- Cities / Counties within the boundaries of the Sabine River Basin (see lists below)
- General and special law districts in accordance with state law, and with the authority and responsibility for water quality protection or solid waste management and located within the Sabine River Basin
- Councils of Government or other governmental entities in the Sabine River Basin

### Water Supply Corporations or Sewer Service Corporations that are:

- Non-profit and member owned
- Audited annually by a certified public accounting firm

### Eligible Counties within the Sabine River Basin:

Collin **	Kaufman **	Sabine
Franklin **	Newton	San Augustine **
Gregg	Orange **	Shelby
Harrison **	Panola	Smith **
Hopkins **	Rains	Upshur **
Hunt **	Rockwall **	Van Zandt **
Jasper **	Rusk **	Wood

\*\* Only partial sections of these counties fall within the Sabine River Basin

### Eligible Cities\*: (Includes Incorporated Cities that fall within the Sabine River Basin)

Alba	Grand Saline	Pine Forest
Beckville	Greenville	Pinehurst
Big Sandy	Hallsville	Point
Bridge City	Hawk Cove	Quinlan
Caddo Mills	Hawkins	Quitman
Campbell	Hemphill	Royse City
Canton	Henderson	Sulphur Springs
Carthage	Huxley	Tatum
Celeste	Joaquin	Tenaha
Center	Josephine	Timpson
Clarksville	Kilgore	Union Grove
Como	Kirbyville	Van
East Mountain	Lakeport	Vidor
East Tawakoni	Lindale	Warren City
Easton	Lone Oak	West Orange
Edgewood	Longview	West Tawakoni
Emory	Marshall	White Oak
Farmersville	Mineola	Wills Point
Fate	Nevada	Winnsboro
Fruitvale	Newton	Winona
Gary	Orange	Yantis
Gladewater	Overton	

\*List was compiled from best available information of current city boundaries, but may not be all inclusive.

<sup>1</sup> Other applicants may be awarded grants at the discretion of the SRA Board of Directors

**Sabine River Authority of Texas Community  
Assistance GRANT Program  
Application Information and Instructions**

**PURPOSE:** The purpose of this program is to provide financial assistance (**GRANT**) for eligible local and regional water resource projects within the Sabine River Basin of Texas, which are consistent with the statutory mission of the Sabine River Authority of Texas (SRA). Created as a conservation and reclamation district in 1949, responsibilities of SRA are to control, store, preserve and distribute the waters of the Sabine River and its tributary system for useful purposes.

**FUNDING:** SRA is prepared to provide funds through a competitive grant process for water resource projects, which include **water supply, wastewater management, water conservation, and water quality**. Grant packages will be reviewed quarterly. **Most grant requests are eligible for up to \$20,000 per project; however, some "shovel-ready" infrastructure or other projects may be considered for more at the discretion of the SRA Board of Directors.**

**Funding Cycles**

- Applications for the Community Assistance Grant Program (CAP-GRANTS) will be reviewed for funding four times a year. Grants may be awarded in **March, July, October and December**. There is no set funding objective for each funding cycle. Projects may be reviewed in one cycle and approved for funding in another cycle. Applications will be kept on file for one year.
- The CAP-GRANTS Review Committee will have the discretion to recommend awarding a grant amount lower than the requested amount.
- The Review Committee will present funding recommendations to the SRA Board of Directors at its quarterly meetings. Awarded applicants will be notified as to the status of their application after Board review.

**ELIGIBLE APPLICANTS:**

**Governmental Entities that are:**

- Cities / Counties within the boundaries of the Sabine River Basin of Texas.
- General and special law districts in accordance with state law, and with the authority and responsibility for water quality protection or solid waste management and located within the Sabine River Basin.
- Councils of Government or other governmental entities in the Sabine River Basin, Texas.

**Water Supply or Sewer Service Corporations that are:**

- Non-profit, member-owned, and member-controlled corporations organized under Chapter 67 of the Texas Water Code.
- Audited annually by a certified public accounting firm. A financial statement may be accepted in lieu of an audit on a case-by-case basis.

*Other applicants may be awarded at the discretion of the SRA Board of Directors.*

**ELIGIBLE PROJECT CATEGORIES:**

- Water Supply – new or existing system improvements
- Wastewater Management – new or existing system improvements
- Water Conservation – measures to promote water use efficiency
- Water Quality – measures to improve instream water quality
- Other – at the discretion of the SRA Board of Directors

**ELIGIBLE COSTS:**

- Feasibility Studies or Reports
- Materials and Supplies
- Construction Costs

**PROJECT REQUIREMENTS:**

- The funds must be used within 12 months of the award date the grant money.
- During the fiscal year funded, the recipient agrees to provide project information to SRA.
- Upon completion of the project, the recipient agrees to notify SRA.

**PROJECT RATING CRITERIA:**

- Match to Mission of SRA
- Location within the Sabine River Basin
- Local Commitment and Support

**Grant funds used with other state or federal funding programs will be given special consideration.**

**APPLICATION INSTRUCTIONS:**

- There are two separate applications in the grant program: 1) Governmental entities, and 2) Water Supply or Sewer Service Corporations. Please type or print all information requested on the appropriate application. Include a daytime phone number for the contact person.
- Please note that Water Supply and Sewer Service Corporation applications have additional information requirements and **require a copy of the most recent audit** (or financial statement) with submittal of the application package.
- **Project Description:** (Additional sheets may be attached to the application if needed) The project description should include **(a)** an overall description and location of the project; **(b)** how the funds from SRA will be used; **(c)** how your project will positively impact or benefit your region, county or city; **(d)** who will maintain the project; **(e)** if applicable, whether or not all other funding sources (state, federal, etc.) have been approved; **(f)** the local commitment and support of the project; **(g)** any in-kind contributions to the project and their dollar value; and **(h)** the timeline of the project showing estimated start-up and completion dates. Specify if the work is required by a schedule imposed by a court order, EPA administrative order, or TCEQ enforcement order.
- Please call CAP Coordinator **Zach Johnson** at **(409) 746-2192** or email **cap@sratx.org** with any questions or for assistance in completing the application.
- **Send one original application and one copy to the address below:**

**Sabine River Authority of Texas  
Community Assistance GRANTS Program  
P. O. Box 579  
Orange, TX 77631**

**Panola County Sexual Assault Response Team  
Report to Commissioners Court  
December 1, 2023**

**1. Introduction**

In 2021 the 87<sup>th</sup> Texas Legislature passed Senate Bill 476. This act required that the Commissioners Court of every county in Texas form an adult Sexual Assault Response Team (SART). The law envisioned an interdisciplinary team consisting of representatives from law enforcement, prosecutors, any sexual assault program within the county, a Sexual Assault Nurse Examiner (SANE), mental or behavioral health providers, and any other professionals that the team considered necessary for operations.

**2. The Panola County Sexual Assault Response Team**

The initial meeting of the Panola County SART was held on April 26<sup>th</sup>, 2022 with the assistance of County Judge David Anderson. The initial members of the SART were:

- 1) Sheriff Sarah Fields, who designated Investigators Hollie Mojica and James Ferris to serve in her absence
- 2) Carthage Police Chief Blake Smith, who designated Detectives Daniel Jones and Carl Harris as his alternate members
- 3) Criminal District Attorney Danny Buck Davidson and his designee, Assistant District Attorney Rick McPherson
- 4) Susan Camazine, RN, a SANE employed by the Rusk-Panola Children's Advocacy Center
- 5) Jerrica Maxey, a victim's advocate with the Women's Center of East Texas, and
- 6) Natalie Smith, a mental health representative of Community Healthcare.

SART meetings are generally scheduled every 90 days, but cancellations are possible due to member availability or a lack of new cases to discuss.

**3. Protocols**

Each discipline has been tasked with preparing their own response protocols or standard operating guidelines. At the time of this report the protocols used by law enforcement and Community Healthcare which are attached separately to this report. As each case is unique and requires its own tailored approach, the guidelines are designed to offer flexibility. Other protocols are still works in progress and will be forwarded to other members and the Court as soon as possible.

**4. Summary of Reports**

Historically sexual assault is one of the most unreported violent crimes that occurs worldwide. Statistics released by the Texas Association Against Sexual Assault (TAASA) indicate that 80% of victims in Texas never report their assaults to law enforcement. One of the goals of the SART concept is to create a more victim-centric approach to investigations and a streamlined care process for survivors. A complicating factor in many of these cases is that reports are sometimes made months or even years after the offense occurred.

Data from the Carthage Police Department is being compiled and will be added as a supplement to this report.

From January 1<sup>st</sup>, 2021-November 30<sup>th</sup>, 2023 the Sheriff's Office received a total of ten reports of sexual assaults involving adult victims. All reports were assigned to an investigator for followup. One case involved an arrest being made after which the victim filed an affidavit of non-prosecution. Two cases were determined to have occurred in other jurisdictions with the case referred to the appropriate agency. One case was closed as unfounded. Two cases were suspended due to victims no longer cooperating with the investigation. One case is still being investigated. No indictments have been returned at this time.

#### 5. Insights and future plans

Quarterly meetings and email updates will continue with SART members. Team members will continue to revise operating protocols and compile data for future reports. The Women's Center of East Texas continues to recruit and train volunteer victim advocates who can accompany victims at the hospital or during interviews.



Attachment A

**Community Healthcare Protocols**

We provide mental health services beyond the scope of what the Women's Center of East Texas or have an immediate crisis. Adult Mental Health Outpatient Services offers behavioral health services including initial intake assessments, medication management, case management, skills training, and counseling to adults age 18 and older with serious mental illness.

Intake: 1-(800)-446-8253

Longview Office: 903-297-1852

Carthage Office: 903-693-7811

**Step-By-Step:**

1. Contact the Intake: they will provide what all the potential client will need as identifiers
  2. Once the intake process is completed they will be linked a case manager or LPC worker to begin services
- **Medication Management:** Scheduled appointments with a provider and assisted with proper medication to enhance recovery (psychiatrist or nurse practitioner)
  - **Skills Training:**
    - Assist clients in identifying and articulating their requests and needs for services and supports.
    - Negotiate and facilitate the array of services and supports needed to address the client's goals and desired outcomes as identified.
    - Provide behavioral intervention services, training and support to assigned caseload.
    - Ensure planned services and supports are implemented
  - **LOC-2 Counseling (EMDR):** One will need to be fit in the eligibility for these services (would be determined in intake assessment)

- **Case Management**: Linking client with resources within the community to enhance recovery, needs, facilitate outside resources. Care Coordination team coming into contact for client to help enhance resource linking.
- **Peer-to-Peer Services**: Another opportunity for clients to enhance social support through having a peer-to-peer worker meeting within them in the reams of Skills Training
- **Crisis Hotline Number**: 1-(800)-832-1009

## Attachment B

### **Law Enforcement Protocols**

Panola County Sheriff's Deputies and Carthage Police Officers will follow their agency policies for responding to calls for service. These are general guidelines to be followed.

- 1). Upon receiving a report of a sexual assault involving an adult victim Dispatch will notify a Patrol Deputy/Officer and the on-call Investigator/Detective. In cases in which a significant period of time has elapsed prior to the report being made an Investigator/Detective will be assigned by their supervisor for followup investigation.
- 2) The assigned Investigator/Detective will be responsible for collecting any evidence including the SANE kit, submitting relevant evidence to the Texas Department of Public Safety crime lab, and updating the kit's process in the DPS Track-Kit system.
- 3) The initial reporting Deputy/Officer or Investigator/Detective will contact the SANE nurse as soon as practical, if a SANE is not immediately available at the local Emergency Room.
- 4) Dispatch will contact the Women's Center hotline to notify a victim advocate.
- 5) Either the reporting Deputy/Officer or Investigator/Detective will complete the request for SANE exam. The reporting Deputy/Officer will provide a case number to the victim.
- 6) As soon as possible the assigned Investigator/Detective will provide a case synopsis to the Criminal District Attorney and work with the prosecution to gather any additional evidence required through subpoenas or search warrants. Once the investigation is completed a full case file will be submitted for prosecution.

7) The Investigator/Detective will present their case before the Grand Jury and testify in the event of a criminal trial. If the original Investigator/Detective is not available when the Grand Jury meets they will be responsible for briefing another officer to present the case.

## Attachment C

### Carthage Police Department Statistics

From January 1<sup>st</sup>, 2021 to present the Police Department received nine reports of adult sexual assaults. All nine cases were investigated. Three indictments were returned.