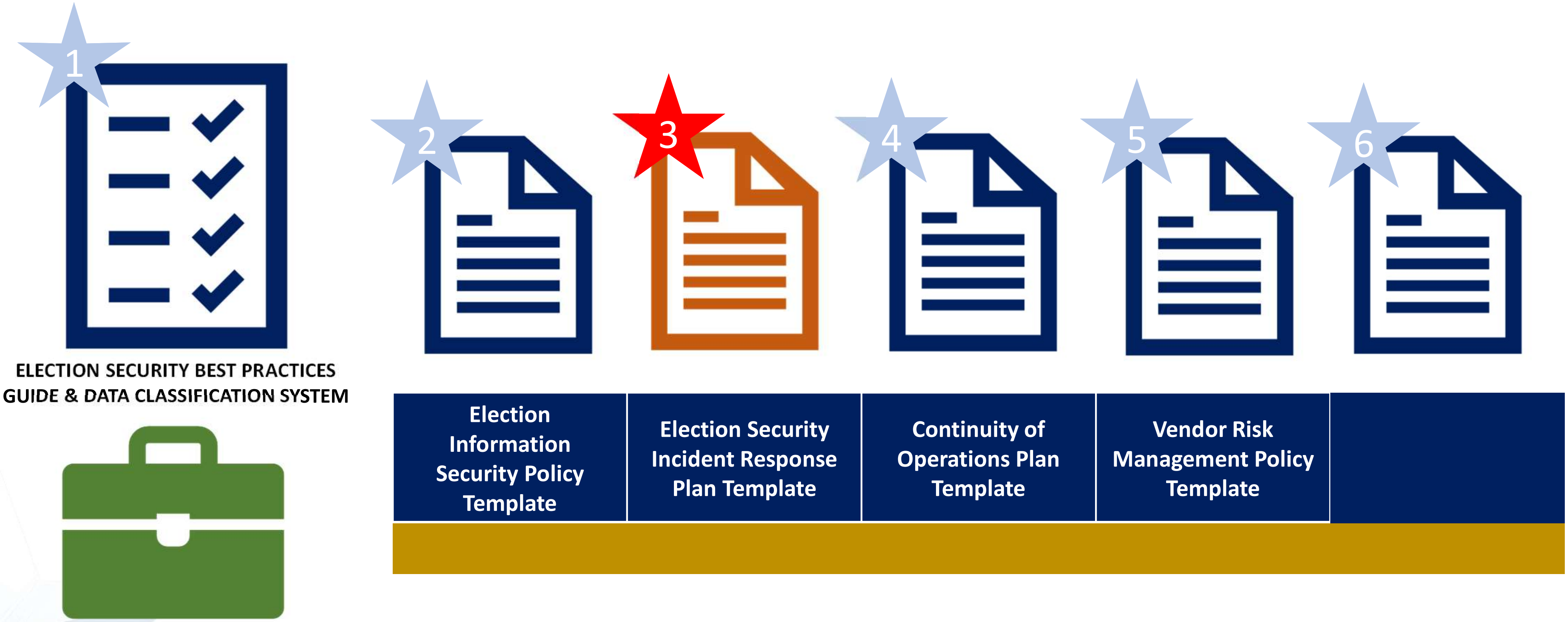
Texas Secretary
of State

Elections Incident Response Plan

WORKSHOP

Texas Secretary of State

ELECTION INCIDENT RESPONSE PLAN



ELECTION SECURITY BEST PRACTICES GUIDE & DATA CLASSIFICATION SYSTEM

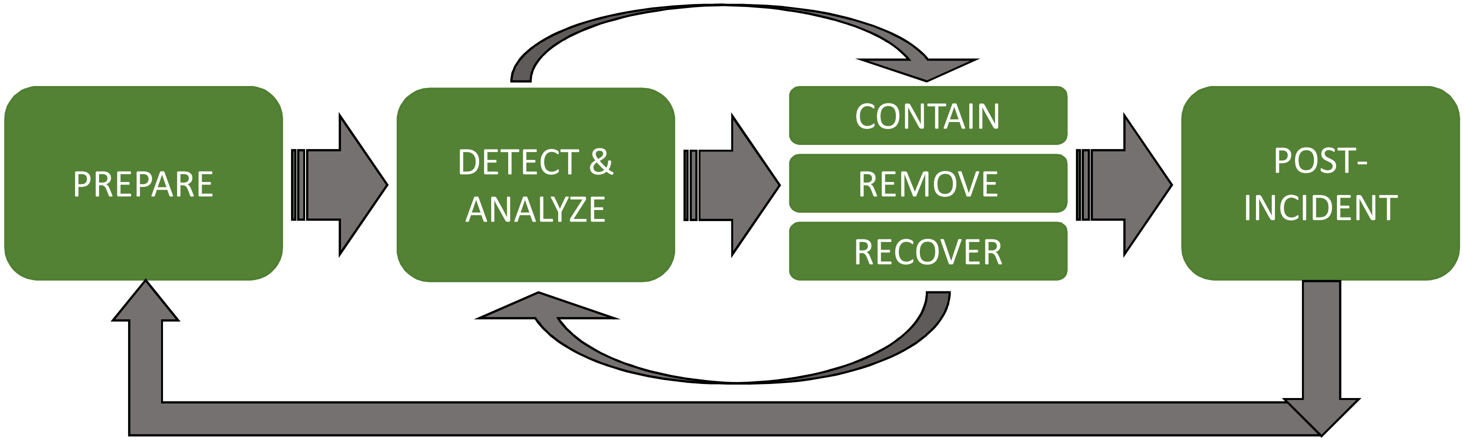
Election Information Security Policy Template

Election Security Incident Response Plan Template

Continuity of Operations Plan Template

Vendor Risk Management Policy Template

Incident Response Cycle



Not a linear process

- Move back and forth between **Detect & Analyze** phase and **Contain, Remove and Recover** phases
- After **Post-Incident** phase, incorporate lessons learned and adjust **Prepare** phase

EIRP Overview: What is it and Why do I need one?

- A detailed step-by-step plan to help you prepare and handle an unexpected incident
- What to do if you ***suspect*** there has been an incident
- What to do once you ***confirm*** there has been an incident
- What to do ***after*** the incident has been handled

When Do I Use It?

When a **sudden** and **unforeseen** incident affecting your operations has been confirmed

Examples may include:

- Voting equipment malfunction
- ePollbooks not operational
- Internet access down
- Tabulation machines down
- Polling locations unusable
- Critical staff unable to perform their duties
- Cybersecurity incident (malware, ransomware, etc.)

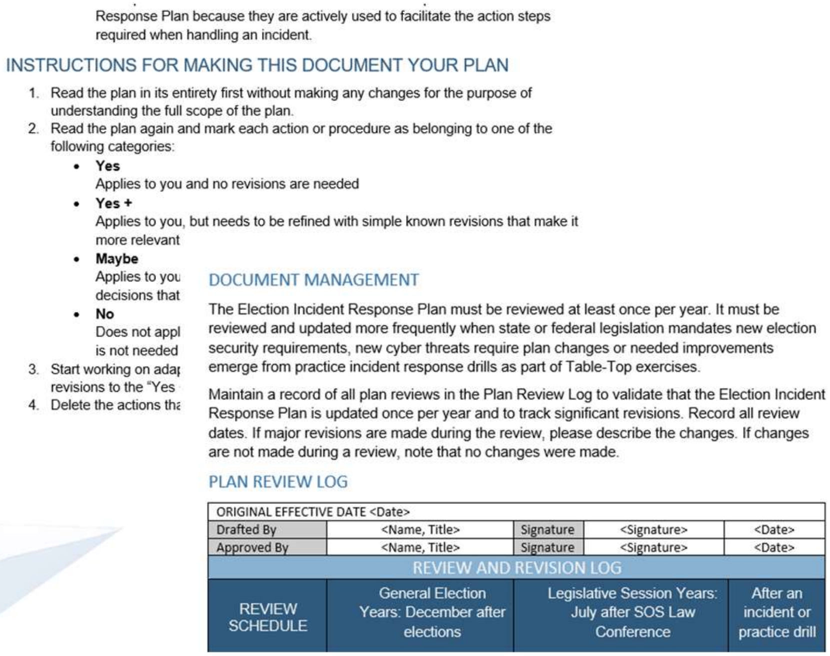
When Do I Use It?

What other examples can you think of?

Have you experienced an incident during an election?

“What do you mean you don’t know where my ballot is?”

Inside The Plan: Guides, Plans, Checklists



Response Plan because they are actively used to facilitate the action steps required when handling an incident.

INSTRUCTIONS FOR MAKING THIS DOCUMENT YOUR PLAN

1. Read the plan in its entirety first without making any changes for the purpose of understanding the full scope of the plan.
2. Read the plan again and mark each action or procedure as belonging to one of the following categories:
   - **Yes**
     Applies to you and no revisions are needed
   - **Yes +**
     Applies to you, but needs to be refined with simple known revisions that make it more relevant
   - **Maybe**
     Applies to you
     decisions that
   - **No**
     Does not appl
     is not needed
3. Start working on adap
   revisions to the "Yes
4. Delete the actions tha

DOCUMENT MANAGEMENT

The Election Incident Response Plan must be reviewed at least once per year. It must be reviewed and updated more frequently when state or federal legislation mandates new election security requirements, new cyber threats require plan changes or needed improvements emerge from practice incident response drills as part of Table-Top exercises.

Maintain a record of all plan reviews in the Plan Review Log to validate that the Election Incident Response Plan 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.

PLAN REVIEW LOG

ORIGINAL EFFECTIVE DATE <Date>				
Drafted By	<Name, Title>	Signature	<Signature>	<Date>
Approved By	<Name, Title>	Signature	<Signature>	<Date>
REVIEW AND REVISION LOG				
REVIEW SCHEDULE	General Election Years: December after elections	Legislative Session Years: July after SOS Law Conference		After an incident or practice drill

- **Thoroughly read** and **review** the template first!!
- Determine what applies to you.
- Gather the required information.
- Assemble a team to discuss and build the template.

Customizing the plan

- Understand the difference between an **event** and **incident.**
- Classify assets and data in order to determine incident severity
- Design plans for potential scenarios.
  - Different situations will require different resources
- Focus on scenarios relevant to your organization.
- Establish reviewing and rehearsing timelines.
- Keep the plan simple.
- Refer to other documents of the Written Information Security Program, if necessary

Customizing the plan

Election Incident Response Plan

- Replace the provided suggestions (underlined, italicized text portions)
- Add your specific instructions (actions, resources, people, methods)
- Fill out information to the best of your ability.

Inside The Plan: Guides, Plans, Checklists

Incident Handler's Log and Report

APPENDIX A

Incident Notification Priority Contact List

APPENDIX B

Incident Response Team Roles and Responsibilities

APPENDIX C

Emergency Contact List

APPENDIX D

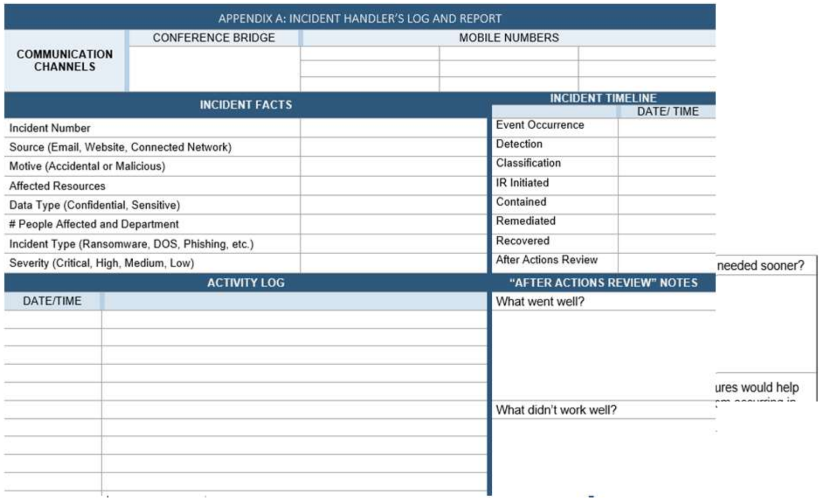
Communications Plan

APPENDIX E

Evidence and Chain of Custody Form

APPENDIX F

Appendix A: Incident Handler’s Log and Report



APPENDIX A: INCIDENT HANDLER’S LOG AND REPORT

	CONFERENCE BRIDGE	MOBILE NUMBERS		
COMMUNICATION CHANNELS				

INCIDENT FACTS	
Incident Number	
Source (Email, Website, Connected Network)	
Motive (Accidental or Malicious)	
Affected Resources	
Data Type (Confidential, Sensitive)	
# People Affected and Department	
Incident Type (Ransomware, DOS, Phishing, etc.)	
Severity (Critical, High, Medium, Low)	

INCIDENT TIMELINE	
	DATE/ TIME
Event Occurrence	
Detection	
Classification	
IR Initiated	
Contained	
Remediated	
Recovered	
After Actions Review	

ACTIVITY LOG

DATE/TIME	

“AFTER ACTIONS REVIEW” NOTES

What went well?

What didn’t work well?

needed sooner?

ures would help

- Living document through the duration of the incident
- Mainly handled by the incident response commander
- Have 10 printed copies available
- Disseminate information in accordance with the communications plan

Inside The Plan: Guides, Plans, Checklists

Incident Handler's Log and Report
APPENDIX A

Incident Notification Priority Contact List
APPENDIX B

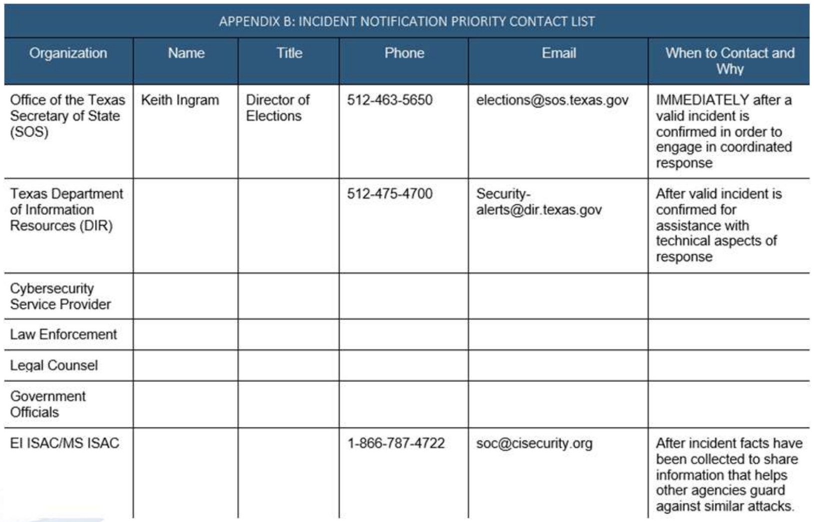
Incident Response Team Roles and Responsibilities
APPENDIX C

Emergency Contact List
APPENDIX D

Communications Plan
APPENDIX E

Evidence and Chain of Custody Form
APPENDIX F

Appendix B: Incident Notification Priority Contact List



APPENDIX B: INCIDENT NOTIFICATION PRIORITY CONTACT LIST

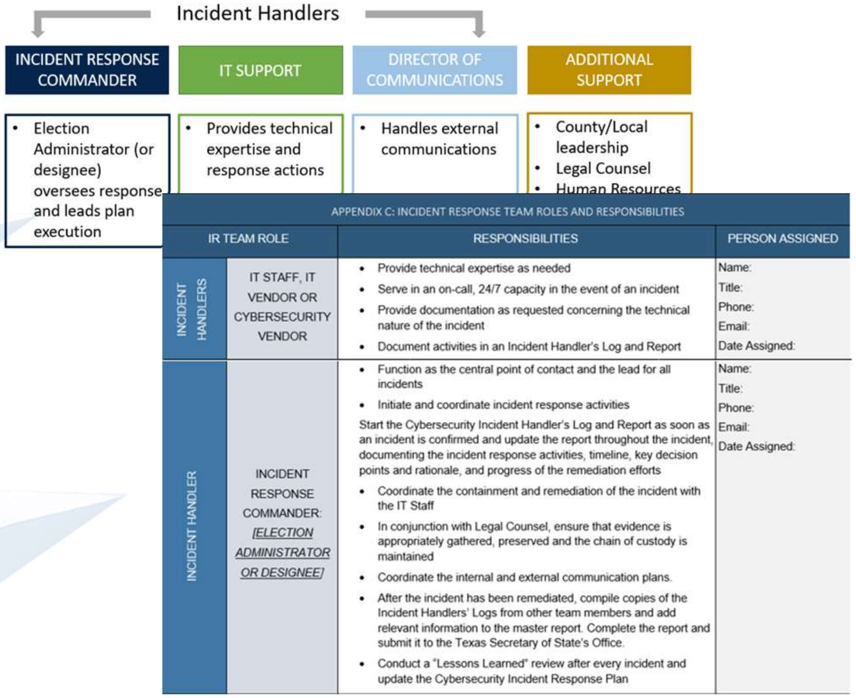
Organization	Name	Title	Phone	Email	When to Contact and Why
Office of the Texas Secretary of State (SOS)	Keith Ingram	Director of Elections	512-463-5650	elections@sos.texas.gov	IMMEDIATELY after a valid incident is confirmed in order to engage in coordinated response
Texas Department of Information Resources (DIR)			512-475-4700	Security-alerts@dir.texas.gov	After valid incident is confirmed for assistance with technical aspects of response
Cybersecurity Service Provider					
Law Enforcement					
Legal Counsel					
Government Officials					
EI ISAC/MS ISAC			1-866-787-4722	soc@cisecurity.org	After incident facts have been collected to share information that helps other agencies guard against similar attacks.

- Notify critical stakeholders (SOS, DIR, CISA, etc.)
- Continue to provide updates periodically or as they occur
- Use official channels for external communications
- Coordinate with emergency management services

Inside The Plan: Guides, Plans, Checklists

- Incident Handler's Log and Report — APPENDIX A
- Incident Notification Priority Contact List — APPENDIX B
- **Incident Response Team Roles and Responsibilities — APPENDIX C**
- Emergency Contact List — APPENDIX D
- Communications Plan — APPENDIX E
- Evidence and Chain of Custody Form — APPENDIX F

Appendix C: EIRP Team Roles and Responsibilities


Incident Handlers

INCIDENT RESPONSE COMMANDER
- Election Administrator (or designee) oversees response and leads plan execution

IT SUPPORT
- Provides technical expertise and response actions

DIRECTOR OF COMMUNICATIONS
- Handles external communications

ADDITIONAL SUPPORT
- County/Local leadership
- Legal Counsel
- Human Resources

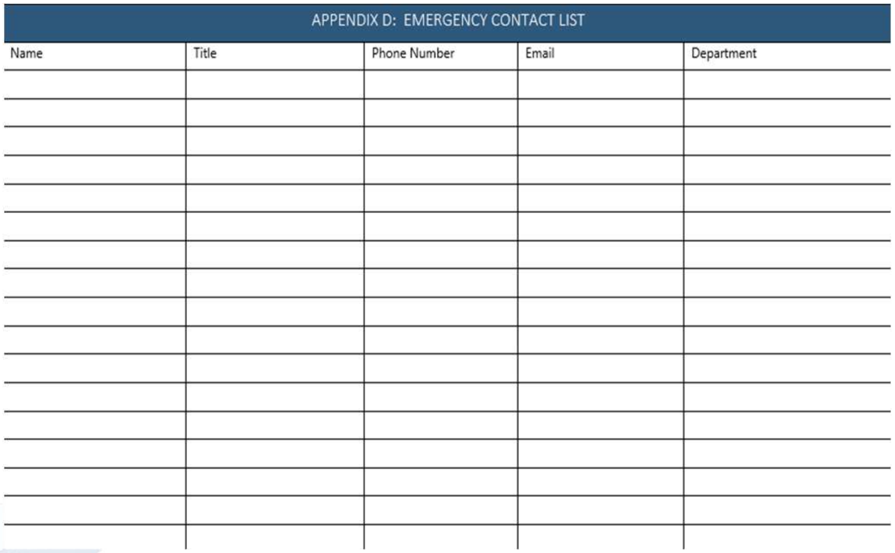
APPENDIX C: INCIDENT RESPONSE TEAM ROLES AND RESPONSIBILITIES			
IR TEAM ROLE		RESPONSIBILITIES	PERSON ASSIGNED
INCIDENT HANDLERS	IT STAFF, IT VENDOR OR CYBERSECURITY VENDOR	• Provide technical expertise as needed • Serve in an on-call, 24/7 capacity in the event of an incident • Provide documentation as requested concerning the technical nature of the incident • Document activities in an Incident Handler's Log and Report	Name: Title: Phone: Email: Date Assigned:
INCIDENT HANDLER	INCIDENT RESPONSE COMMANDER: *[ELECTION ADMINISTRATOR OR DESIGNEE]*	• Function as the central point of contact and the lead for all incidents • Initiate and coordinate incident response activities 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 • Coordinate the containment and remediation of the incident with the IT Staff • In conjunction with Legal Counsel, ensure that evidence is appropriately gathered, preserved and the chain of custody is maintained • Coordinate the internal and external communication plans. • 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. • Conduct a "Lessons Learned" review after every incident and update the Cybersecurity Incident Response Plan	Name: Title: Phone: Email: Date Assigned:

- Ensure team members know their responsibilities.
- Conduct rehearsals (planned or unplanned)
- Establish a secure way to communicate the team members once plan has been activated

Inside The Plan: Guides, Plans, Checklists

- Incident Handler's Log and Report — APPENDIX A
- Incident Notification Priority Contact List — APPENDIX B
- Incident Response Team Roles and Responsibilities — APPENDIX C
- **Emergency Contact List** — APPENDIX D
- Communications Plan — APPENDIX E
- Evidence and Chain of Custody Form — APPENDIX F

Appendix D: Emergency Contact List



APPENDIX D: EMERGENCY CONTACT LIST

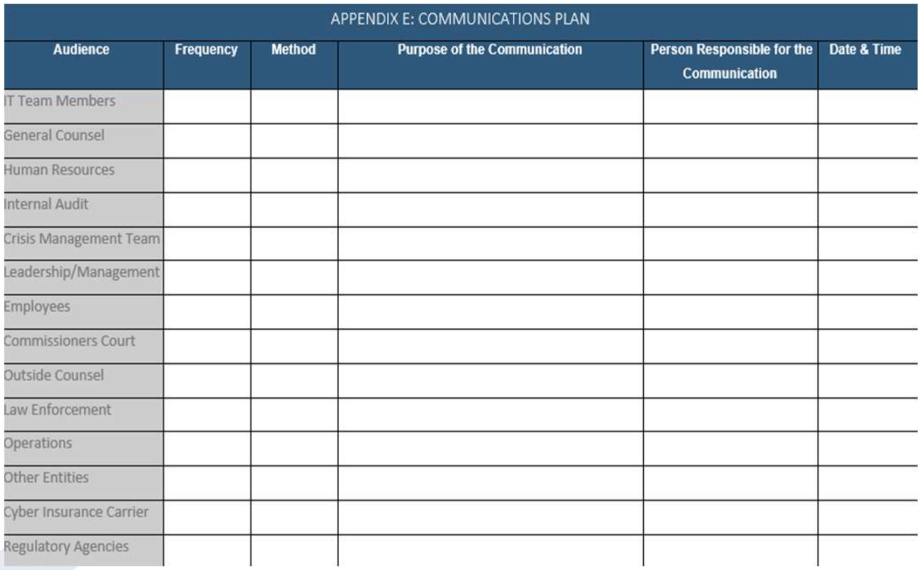
Name	Title	Phone Number	Email	Department

- List with internal staff contact information
- Delegate updates to department managers
- Notify your internal staff about the incident

Inside The Plan: Guides, Plans, Checklists

- Incident Handler's Log and Report — APPENDIX A
- Incident Notification Priority Contact List — APPENDIX B
- Incident Response Team Roles and Responsibilities — APPENDIX C
- Emergency Contact List — APPENDIX D
- **Communications Plan** — APPENDIX E
- Evidence and Chain of Custody Form — APPENDIX F

Appendix E: Communications Plan



APPENDIX E: COMMUNICATIONS PLAN

Audience	Frequency	Method	Purpose of the Communication	Person Responsible for the Communication	Date & Time
IT Team Members					
General Counsel					
Human Resources					
Internal Audit					
Crisis Management Team					
Leadership/Management					
Employees					
Commissioners Court					
Outside Counsel					
Law Enforcement					
Operations					
Other Entities					
Cyber Insurance Carrier					
Regulatory Agencies					

- Maintain information flow through communications director
- Communicate incident details on a need-to-know basis

Inside The Plan: Guides, Plans, Checklists

Incident Handler's Log and Report

APPENDIX A

Incident Notification Priority Contact List

APPENDIX B

Incident Response Team Roles and Responsibilities

APPENDIX C

Emergency Contact List

APPENDIX D

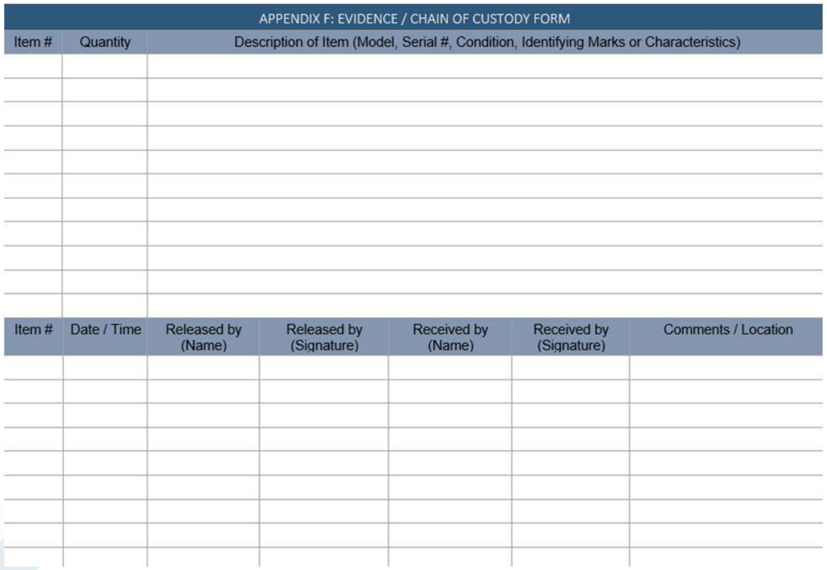
Communications Plan

APPENDIX E

Evidence and Chain of Custody Form

APPENDIX F

Appendix F: Evidence and Chain of Custody form



APPENDIX F: EVIDENCE / CHAIN OF CUSTODY FORM

Item #	Quantity	Description of Item (Model, Serial #, Condition, Identifying Marks or Characteristics)

Item #	Date / Time	Released by (Name)	Released by (Signature)	Received by (Name)	Received by (Signature)	Comments / Location

- Enter as much detail as possible
- Maintain copies of produced forms
- Provide copies to insurance/vendors, if applicable

Final Thoughts

- Three components to Incident Response: **Plan, Team, Tools.**
- **Interoperability** with other documents

AVAILABLE SUPPORT

WEBINARS

TRAINING

RESOURCES

ELECTION SECURITY TRAINERS
ElectionSecurity@sos.texas.gov

Q&A