IS PROJECT

ELECTION SECURITY POLICY AND ANSWERS TO 70 INFORMATION SECURITY QUESTIONS

Group Members:

BILAL AHMED KHAN [K200183] | MUHAMMAD ABDULLAH JAWED [K201689] | MUAAZ ALAM [K200212]

Contents

Answers of 70 questions related to risk assessment

Introduction

The answer the 70 questions to assess security risk with respect to election activity in Pakistan is given below, the information is taken from official handouts provided by Election commission of Pakistan to DRO (District Returning Officers), RO (Returning Officers) and Election Act 1974. [All of the aforementioned documents are submitted with the report].

Training

According to the handbook issued for District returning officers by Election Commission Pakistan (available on official website:https://ecp.gov.pk/training-material) it is an integral part of pre-poll preparation of elections to provide adequate training to the polling staff which also encompasses training them w.r.t. the security aspect of the elections.

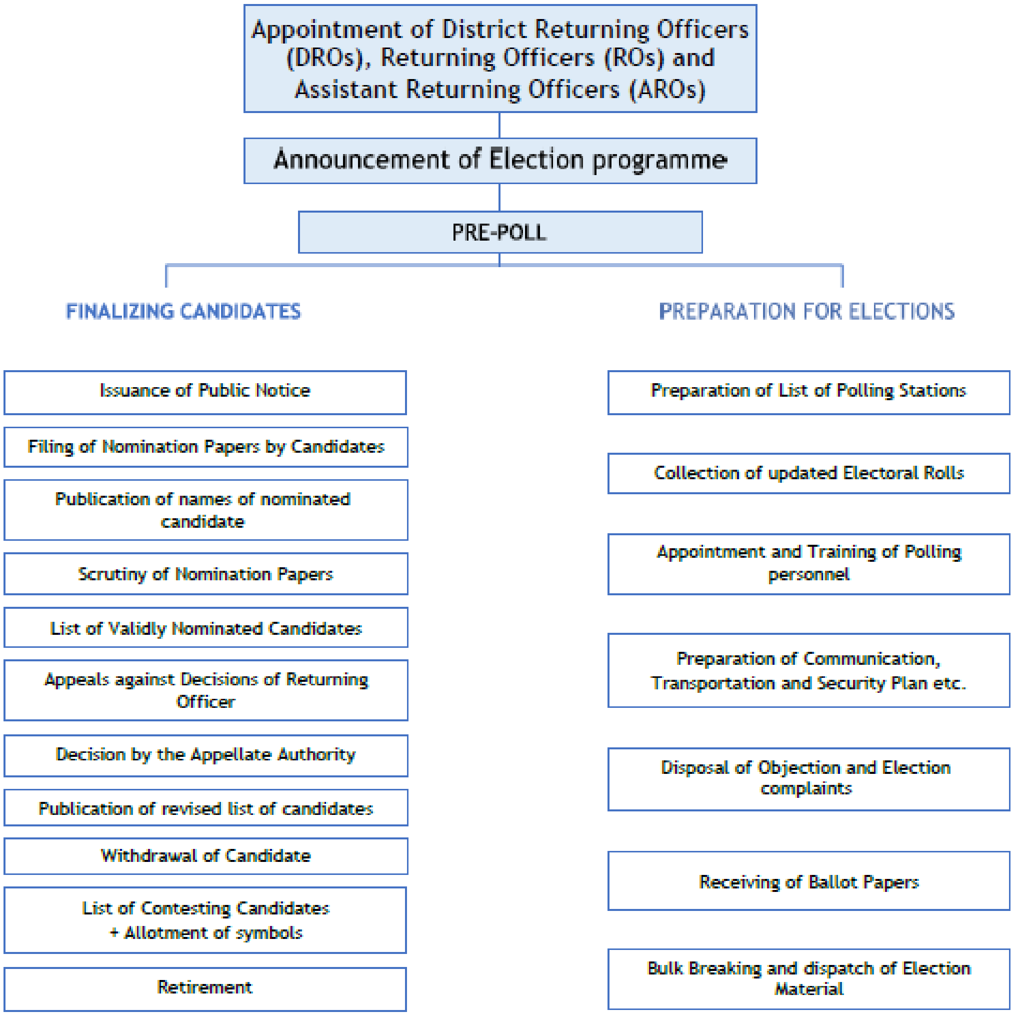
Appointment of District Returning Officers (DROs), Returning Officers (ROs) and Assistant Returning Officers (AROs)
Announcement of Election programme
PRE-POLL
FINALIZING CANDIDATES
PREPARATION FOR ELECTIONS
Issuance of Public Notice
Filing of Nomination Papers by Candidates
Publication of names of nominated candidate
Scrutiny of Nomination Papers
List of Validly Nominated Candidates
Appeals against Decisions of Returning Officer
Decision by the Appellate Authority
Publication of revised list of candidates
Withdrawal of Candidate
List of Contesting Candidates + Allotment of symbols
Retirement
Preparation of List of Polling Stations
Collection of updated Electoral Rolls
Appointment and Training of Polling personnel
Preparation of Communication, Transportation and Security Plan etc.
Disposal of Objection and Election complaints
Receiving of Ballot Papers
Bulk Breaking and dispatch of Election Material

Figure 1 Pre-Poll Electoral Process

The diagram above provides a detailed overview of the prepoll activities that need to be performed by the DRO (District Returning Officer). Preparing for the communication, transportation and Security Plan are an integral part of preparing for the elections.

A/c to the DRO handbook issued the ECP, "**Ensuring that proper security, Transportation and Communication plan etc. is in place for safe transportation of election material and staff to the polling station and communication of result to the ECP.** " is a prime responsibility of the District Returning Officer.

The presiding officer must, "**Take a full review of all security arrangements at polling station and only allow authorized persons i.e candidates, polling agents, election agent or persons having Accreditation Card from the Election Commission, the DRO or RO to enter the polling station other than voters.**"

Access Control

According to the DRO handbook issued by ECP only, "**Election agent nominated by the candidate is authorized to access all the polling stations of the relevant constituency.**"

The Elections Act of 1974 in Pakistan primarily focuses on the legal and procedural aspects of elections rather than the technical details of access control during the electoral process. However, the security and access control measures during elections in Pakistan involve a combination of legal provisions, administrative practices, and technical measures to ensure the integrity of the electoral process.

The Elections Act and other relevant laws empower the Election Commission of Pakistan (ECP) to regulate and oversee the electoral process, including access to polling stations and counting centers.

Access control is maintained through the deployment of law enforcement personnel at polling stations and other election-related facilities. They are responsible for ensuring that only authorized individuals, such as voters, election officials, and accredited observers, are allowed entry.

Access to the voting process is controlled through the maintenance of accurate voter lists. Only registered voters are allowed to cast their votes, and a proper identification process is in place to verify the identity of voters.

End User (Voter)

In order to educate the voter about the vote casting process, ECP conducts various voter awareness programs such as ECP Voter outreach program.

Furthermore, in order to verify the authenticity of the voter ECP takes the following steps:

- The Election Commission maintains updated voter lists, and only individuals whose names appear on these lists are eligible to vote. This list is a crucial tool for verifying the eligibility of voters.
- Voters are typically required to present their National Identity Cards (NICs) at the polling stations for identification. The NIC is a widely recognized official identification document in Pakistan.

The handbook for returning officers (RO) issued by the ECP (available on official website: https://ecp.gov.pk/training-material) also outlines the following principles for voter facilitation and ensuring the correct casting of votes.

- There should be no factor influencing the voters' choice on poll day.
- Each polling station will consist of 2-4 polling booths (depending on the number of voters assigned to each polling station).
- The Presiding Officer must ensure that Computerized Pictorial Electoral Roll (with photograph of voters) provided by the Returning Officer is used at the polling station.
- Ensuring that only voters registered on the Electoral Roll, are permitted to vote.
- Ensuring placement of Screened off Compartments at appropriate place so that secrecy of each voter is ensured.
- Take a full review of all security arrangements at polling station and only allow authorized persons i.e candidates, polling agents, election agent or persons having Accreditation Card from the Election Commission, the DRO or RO to enter the polling station other than voters.

End Points (Polling Station)

In order to secure the polling stations and to ensure seamless conduction of elections the ECP handbooks prescribes the DRO to, "**declare Polling stations as highly sensitive, in consultation with head of District Police.**"

It is the responsibility of the DRO to, "**Ensure that proper security, Transportation and Communication plan etc. is in place for safe transportation of election material and staff to the polling station and communication of result to the ECP.**"

Furthermore, the official handbook of ECP also instructs to,

"Appointing impartial polling staff at the polling stations. Submission of the list of polling staff (Presiding Officers, Assistant Presiding Officers and Polling Officers) appointed for the conduct of election, to the DRO (at least 14 days before the poll day) for approval."

The election Act 1974 has the following guidelines with respect to securing the polling stations on election day,

- Polling stations are designated as restricted areas during elections. Only authorized individuals, such as voters, election officials, and accredited observers, are allowed entry. Unauthorized individuals are restricted from entering the polling premises.
- Election officials and polling staff are trained to follow security protocols. They are briefed on procedures to handle potential security threats and emergencies.
- The Act or associated rules specify procedures for the sealing and opening of ballot boxes. This is done in a secure manner to prevent tampering and maintain the secrecy of the vote.
- Strict procedures for voter identification are often in place to prevent impersonation and ensure that only eligible voters cast their ballots. This may include the verification of National Identity Cards (NICs) and, in some cases, the use of biometric verification.
- ECP may invite local and international election observers to monitor the electoral process. Their presence contributes to transparency and can act as a deterrent to irregularities.

The Presiding Officer will act as Magistrate of the First Class as authorized by the Commission and will be responsible to maintain law and order at the polling station.

Security Architecture

The Election Commission of Pakistan, employs security best practices to safeguard their systems and data.

1. Principle of Least Privilege:

The DRO handbook issued by the ECP states that, **"Election Agent must adhere to the principle of non-interference."**

2. Zero Trust Model:

The election model in Pakistan also relies on independent observers to approve the elections, this can be termed as an iteration of zero trust model.

According to the DRO handbook independent observers perform the following actions during elections:

1. Observing all stages of the polling process, except stamping of a ballot paper by a voter.
2. Observer is not allowed to speak to any polling staff which may hinder their work.
3. Observing the counting of vote and if he/ she intends, sign the Result of the Count (Form-XI) and Ballot Paper Account (Form-XII).

3. Multifactor Authentication (MFA):

MFA is incorporated in the security model at various staged such as the official DRO handbook states that the District Returning Officer has the authority to issue accreditation cards to observers and media persons.

DRO should ensure that the applicant has provided requisite documents such as:

- Written application on letter head of organization along with details in respect of name, contact number and address of the observer.
- Letter from media house in case the applicant is from print or electronic media
- Two recent colored photographs and a photocopy of valid NIC

No person shall be allowed to observe the conduct of election, if he:

- is not accredited as an observer by the Commission or its authorized officer;
- is affiliated with any political party;
- fails to provide his full particulars and documents, including photographs;
- has been involved in activities prejudicial to the peace and tranquility of the people of a constituency;
- fails to provide an authorization from the organization of which he is a member.

4. Credential Management:

The Presiding officer must take a full review of all security arrangements at polling station and only allow authorized persons i.e candidates, polling agents, election agent or persons having Accreditation Card from the Election Commission, the DRO or RO to enter the polling station other than voters.

Cryptography:

Enforcing the imperative need for comprehensive cryptographic safeguards, the Electoral Rolls Act of 1974 in Pakistan mandates the protection of sensitive electoral data. The Act accentuates the significance of robust key management practices, encompassing key generation, storage, usage, and destruction. The storage of cryptographic keys in minimal locations, preferably secure hardware modules or dedicated key vaults, is underscored. Dual custodianship, requiring the presence of two authorized individuals for key access and usage, is advocated. To fortify data protection, the Act recommends the utilization of full disk encryption on all relevant drives, ensuring the prevention of unauthorized access even if the physical device is lost or stolen. Emphasizing the crucial role of encryption in safeguarding data in transit, the Act insists on the use of strong encryption protocols like Transport Layer Security (TLS) 1.1 or higher during the transfer of electoral data over networks. Non-console administrative access to electoral systems should employ robust cryptography mechanisms, such as Secure Shell (SSH) or VPN protocols, safeguarding sensitive administrative activities from unauthorized access and interception. Through these comprehensive cryptographic measures, the Electoral Rolls Act aims to secure the confidentiality, integrity, and availability of electoral data, fostering a trustworthy electoral process.

Threats:

While the Electoral Rolls Act of 1974 in Pakistan doesn't explicitly address threat mitigation strategies, it underscores the vital need to safeguard electoral data from evolving cybersecurity threats. Extending its principles, proactive threat hunting, comprehensive threat intelligence integration, and vigilant monitoring of vendor and third-party supply chains are emphasized. Conducting targeted threat hunts is crucial for identifying and neutralizing potential cybersecurity threats before compromising electoral systems. Ingesting current threat intelligence from multiple sources is essential to stay abreast of emerging cybersecurity threats, informing vulnerability management, security incident response planning, and proactive threat hunting efforts. Routine dark web reconnaissance is vital for uncovering information about the organization's brand and structures that may be exploited by malicious actors. Closely monitoring vendor and third-party supply chain connections ensures external entities do not pose security risks to electoral systems. Implementing these comprehensive threat mitigation strategies enhances the cybersecurity posture of organizations responsible for electoral data, safeguarding the integrity of the electoral process.

Testing:

Mandating rigorous testing procedures, the Electoral Rolls Act of 1974 in Pakistan underscores the importance of ensuring the security of electoral systems and data. The Act emphasizes regular penetration testing, vulnerability scanning, business impact analysis, and the formulation of comprehensive security policies. To address potential vulnerabilities, the Act recommends at least one annual penetration test by a qualified third-party organization, simulating real-world attacks to proactively identify and remediate security weaknesses. Routine vulnerability scans are crucial for maintaining a secure environment, advocating scanning all systems regularly to detect and prioritize vulnerabilities based on their Common Vulnerability Scoring System (CVSS) score. Business impact analysis, conducted annually, assists in assessing the potential impact of cyberattacks and developing mitigation strategies. Through these testing measures, the Electoral Rolls Act aims to fortify electoral systems against potential security threats.

Policy:

Emphasizing the need for robust security policies, the Electoral Rolls Act of 1974 in Pakistan mandates the implementation of an enterprise security policy reviewed and updated at least annually. This policy is expected to define security guidelines, procedures, and responsibilities for all users and systems. Additionally, the Act advocates for a formal change control policy outlining the process for approving and implementing changes to systems, ensuring security considerations are incorporated into all change requests. By adhering to formal change control processes, organizations minimize the risk of introducing vulnerabilities into their systems. Through these testing and policy measures, the Electoral Rolls Act strives to create a secure and resilient electoral environment capable of withstanding increasing cyber threats.

Physical:

Highlighting the significance of robust physical security measures, the Electoral Rolls Act of 1974 in Pakistan underscores the importance of protecting electoral data and infrastructure. The Act advocates for restricting physical access to critical systems and equipment, controlling the use of publicly accessible network jacks, and establishing clear procedures for visitor access. To secure servers, consoles, backup devices, and network equipment, the Act recommends implementing physical security measures like access control systems, secure perimeter barriers, and surveillance cameras. These controls need proper maintenance and regular testing to ensure their effectiveness in preventing unauthorized access. Logical controls, such as port filtering and network segmentation, are proposed to control the use of publicly accessible network jacks, restricting unauthorized access to the network and preventing malicious actors from gaining access to sensitive electoral data. Additionally, the Act mandates the establishment of clear procedures for visitor access, requiring authorized personnel escorting visitors at all times, granting access only to authorized areas, and maintaining a log of their activities. By implementing comprehensive physical security measures, the Electoral Rolls Act aims to safeguard electoral systems and data from unauthorized physical access, ensuring the integrity and confidentiality of electoral processes.

Plans:

Mandating the implementation and regular review of a comprehensive cyber incident response plan (CIRP), the Electoral Rolls Act of 1974 in Pakistan emphasizes the need for clear procedures to identify, contain, eradicate, and recover from cyberattacks. The core and extended incident response teams are expected to practice their response capabilities at least annually using tabletop or functional cybersecurity exercises. These exercises ensure that the teams are prepared to respond effectively to real-world cyberattacks. By enforcing the development and practice of a CIRP, the Electoral Rolls Act aims to enhance the readiness and resilience of electoral systems against cyber threats.

Inventory:

The importance of maintaining accurate and up-to-date network diagrams and asset inventories is underscored by the Electoral Rolls Act of 1974 in Pakistan. These diagrams and inventories should provide a comprehensive overview of the organization's IT infrastructure, including WiFi networks, all hardware and software assets, and their respective owners and co-owners. This information is deemed crucial for effective asset management, cybersecurity incident response, and disaster recovery. Additionally, the Act recommends maintaining a complete set of data flow diagrams to visualize the movement of data within the organization and identify potential vulnerabilities or security gaps. Through meticulous inventory management, the Electoral Rolls Act aims to ensure a robust foundation for cybersecurity practices and response strategies.

Data Management:

Emphasizing robust data management practices, the Electoral Rolls Act of 1974 in Pakistan advocates for measures to protect the confidentiality, integrity, and availability of electoral data. The Act recommends utilizing file integrity monitoring (FIM) for critical data, minimizing storage of confidential data, implementing data classification, deploying data loss prevention (DLP) solutions, and preventing data transfer to unauthorized devices. To safeguard the organization's "crown jewels," the Act recommends employing FIM solutions that continuously monitor file changes and alert administrators to any unauthorized modifications, ensuring the unaltered and protected status of critical data. The Act also stresses the importance of minimizing the storage of confidential data, with organizations establishing data retention policies to define the timeframe for storing different types of data and mandate secure deletion when no longer needed. Advocating for data classification throughout the network, the Act involves assigning sensitivity levels to different data types, allowing prioritized protection efforts and implementation of appropriate security controls based on data sensitivity. To prevent unauthorized data loss, the Act recommends deploying DLP solutions, which monitor and control data movement across the network and cloud environments, preventing confidential data from being transferred to unauthorized locations or accessed by unauthorized individuals. Additionally, the Act mandates preventing confidential data from being copied to external devices and restricting the use of external devices on endpoints, achieved through endpoint device controls. By implementing these comprehensive data management practices, the Electoral Rolls Act aims to fortify the protection of electoral data against unauthorized access and data breaches.

Software Development:

Underlining the importance of secure software development practices, the Electoral Rolls Act of 1974 in Pakistan advocates for defining and implementing processes and mechanisms to minimize vulnerabilities and protect electoral systems from cyberattacks. The Act recommends integrating secure coding practices, code reviews, vulnerability scanning, and penetration testing into the software development lifecycle (SDLC) to address security considerations throughout the development process. It further encourages the employment of software engineering techniques designed to prevent and mitigate common software attacks, focusing on input validation, error handling, secure data storage, and access control mechanisms. For public-facing web applications, the Act stresses ongoing threat monitoring and vulnerability remediation. Organizations are prompted to establish processes for identifying, assessing, and prioritizing new threats and vulnerabilities, promptly implementing patches and updates to address these risks. The Act advocates for a layered security approach for public-facing web applications, including firewalls, intrusion detection systems, and web application firewalls to block or detect malicious traffic and prevent unauthorized access to sensitive data. Enforcing segregation between preproduction and production environments is mandated to minimize the risk of introducing vulnerabilities. Through these measures, the Electoral Rolls Act aims to bolster the security of electoral systems against potential software-related vulnerabilities and cyber threats.

Mobile Devices:

Highlighting the importance of effective mobile device management, the Electoral Rolls Act of 1974 in Pakistan emphasizes the need to protect electoral data from unauthorized access and loss. The Act advocates for implementing comprehensive MDM policies that address device registration, application management, data encryption, and remote wipe capabilities. These policies should clearly define the acceptable use of mobile devices and enforce security measures to protect sensitive electoral data. Disallowing any connectivity of mobile devices not controlled by enterprise security mechanisms is mandated, ensuring only authorized and managed devices can access electoral systems and preventing unauthorized access from compromised or uncontrolled devices. To further enhance the protection of electoral data on mobile devices, the Act recommends implementing additional security controls, such as strong password requirements,

Security Policy for Election Activities

Introduction:

In the dynamic landscape of contemporary democracies, the integrity of electoral processes is fundamental to ensuring the voice of the people is accurately represented. This comprehensive security policy for election activities in Pakistan serves as a meticulous blueprint, addressing multifaceted aspects of security ranging from access control procedures to advanced cryptography measures and proactive threat mitigation strategies. Grounded in principles such as the Principle of Least Privilege and the Zero Trust Model, this policy reflects a commitment to safeguarding the electoral infrastructure against potential threats. By integrating technology, education, and strategic planning, this aims to fortify the democratic foundation of the nation, fostering trust in the electoral system among citizens, candidates, and international observers alike.

1. Access Control Procedures:

1.1 Election Agent Access

Only Election Agents nominated by candidates are granted access to all polling stations of the relevant constituency. To ensure compliance, the Election Commission will maintain a centralized database of authorized Election Agents, accessible by District Returning Officers (DROs) and Returning Officers (ROs).

1.2 Voter Access:

Access to the voting process will be strictly controlled by maintaining accurate and up-to-date voter lists. The Election Commission will leverage advanced database management systems to ensure the integrity and accuracy of voter information. Identification at polling stations will be facilitated through the mandatory presentation of National Identity Cards (NICs), which will undergo real-time verification against the central database.

1.3 Observer Access:

Independent observers play a critical role in ensuring the transparency and fairness of elections. The accreditation process for observers will involve a rigorous verification procedure conducted by the District Returning Officer. Accreditation cards will be equipped with secure QR codes for authentication at polling stations, providing an additional layer of security.

1.4 Credential Management:

Credential management is paramount for controlling access to sensitive areas. The issuance of accreditation cards by the Election Commission, DROs, or ROs will be a meticulous process. Access will be granted only to individuals with a valid reason, such as candidates, polling agents, election agents, or those holding authorized Accreditation Cards.

2. End-User (Voter) Procedures:

2.1 Voter Education:

Voter awareness programs will be conducted regularly to educate voters about the voting process, emphasizing the importance of fair and unbiased decision-making.

2.2 Voter Verification:

The Election Commission will maintain an updated and secure voter registration system. Voters will be required to present their National Identity Cards (NICs) for verification, and any discrepancies will be addressed promptly.

2.3 Polling Station Procedures:

The use of Computerized Pictorial Electoral Rolls with screened off compartments will ensure the secrecy of each voter.

Regular reviews of security arrangements at polling stations will be conducted by the Presiding Officer to identify and address any potential vulnerabilities.

3. Security Architecture:

3.1 Principle of Least Privilege:

Election Agents must strictly adhere to the principle of non-interference, ensuring that their actions do not compromise the integrity of the electoral process.

3.2 Zero Trust Model:

The Election Commission will implement a Zero Trust Model, considering all entities, even those within the organization, as potentially untrusted. This approach ensures continuous verification and validation of activities throughout the election process.

3.3 Multifactor Authentication (MFA):

Multifactor Authentication (MFA) will be incorporated into the security model, particularly in the issuance of accreditation cards to observers and media persons. The District Returning Officer will verify the applicant's identity using multiple factors, including written applications, letters from media houses, photographs, and a photocopy of a valid NIC.

4. Cryptography Procedures:

4.1 Key Management:

The Electoral Rolls Act of 1974 mandates robust key management practices. The Election Commission will implement a secure key generation, storage, usage, and destruction process, minimizing the locations where cryptographic keys are stored and enforcing dual custodianship for key access.

4.2 Data Encryption:

To safeguard sensitive electoral data, the Act recommends the use of full disk encryption on all relevant drives. Additionally, during the transfer of electoral data over networks, strong encryption protocols like TLS 1.1 or higher will be employed to ensure confidentiality and integrity.

5. Threat Mitigation Strategies:

5.1 Proactive Threat Hunting:

The Election Commission will establish a dedicated team for proactive threat hunting. This team will continuously monitor for potential threats, integrating comprehensive threat intelligence to stay ahead of emerging cybersecurity risks.

5.2 Vendor and Supply Chain Monitoring:

A robust vendor and supply chain monitoring program will be implemented to ensure that external entities do not pose security risks to electoral systems. The Election Commission will conduct regular assessments of vendors and third-party connections to identify and address potential vulnerabilities.

6. Physical Security Measures:

6.1 Access Restrictions:

To prevent unauthorized physical access, the Election Commission will implement access controls, secure perimeter barriers, and surveillance cameras. Restricted access zones will be clearly demarcated, and only authorized personnel will be granted access.

6.2 Visitor Procedures:

Clear procedures for visitor access will be established, requiring authorized personnel to escort visitors at all times. Access will be granted only to authorized areas, and a detailed log of visitor activities will be maintained for auditing purposes.

7. Inventory Management:

7.1 Network Diagrams and Asset Inventories:

Accurate and up-to-date network diagrams and asset inventories will be maintained, providing a comprehensive overview of the organization's IT infrastructure. These diagrams and inventories will specifically include information relevant to the election systems outlined in the methodology and the 70 questions.

7.2 Data Flow Diagrams:

A complete set of data flow diagrams will be maintained to visualize the movement of data within the organization, specifically focusing on the data flow related to election systems. This will help identify potential vulnerabilities or security gaps in the electoral data management process.

8. Data Management Practices:

8.1 File Integrity Monitoring (FIM):

File Integrity Monitoring (FIM) solutions will be employed to continuously monitor critical electoral data for file changes. Any unauthorized modifications will trigger alerts, ensuring the unaltered and protected status of critical data, as outlined in the methodology.

8.2 Data Classification and DLP:

Data classification will be implemented throughout the network, assigning sensitivity levels to different data types. This approach will guide prioritized protection efforts and the implementation of appropriate security controls based on data sensitivity. Data Loss Prevention (DLP) solutions will be deployed to monitor and control data movement, preventing unauthorized access and data breaches.

9. Software Development Security:

9.1 Secure Software Development Practices:

Secure coding practices, code reviews, vulnerability scanning, and penetration testing will be integrated into the Software Development Lifecycle (SDLC). These practices will specifically address security considerations related to the development and maintenance of election systems.

9.2 Web Application Security:

Public-facing web applications related to election systems will undergo ongoing threat monitoring and vulnerability remediation. A layered security approach, including firewalls, intrusion detection systems, and web application firewalls, will be implemented to block or detect malicious traffic and prevent unauthorized access to sensitive electoral data.

10. Mobile Device Management:

10.1 MDM Policies:

Comprehensive Mobile Device Management (MDM) policies will be implemented, specifically addressing device registration, application management, data encryption, and remote wipe capabilities for devices used in the context of election activities.

10.2 Mobile Device Connectivity:

To enhance the protection of electoral data on mobile devices, only authorized and managed devices will be allowed to access electoral systems. Any connectivity not controlled by enterprise security mechanisms will be disallowed, preventing unauthorized access from compromised or uncontrolled devices.