**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.

5.3 Dark Web Reconnaissance:

Routine dark web reconnaissance will be conducted to uncover information about the organization's brand and structures that may be exploited by malicious actors. This proactive approach will enable the Election Commission to mitigate potential threats before they materialize.

6. Testing Procedures:

6.1 Penetration Testing:

To identify and address security weaknesses, the Election Commission will conduct at least one annual penetration test by a qualified third-party organization. This test will simulate real-world cyberattacks to proactively assess and enhance the security posture of electoral systems.

6.2 Vulnerability Scanning:

Regular vulnerability scans will be performed on all systems to detect and prioritize vulnerabilities based on their Common Vulnerability Scoring System (CVSS) score. This systematic approach will enable the timely remediation of identified vulnerabilities, reducing the risk of exploitation.

7. Policy Implementation:

7.1 Enterprise Security Policy:

The Election Commission will implement a comprehensive enterprise security policy, reviewed and updated annually. This policy will define clear security guidelines, procedures, and responsibilities for all users and systems involved in the electoral process.

7.2 Change Control Policy:

A formal change control policy will be adhered to, outlining the process for approving and implementing changes to systems. This policy will ensure that security considerations are incorporated into all change requests, minimizing the risk of introducing vulnerabilities.

8. Physical Security Measures:

8.1 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.

8.2 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.

9. Incident Response Plan:

9.1 Cyber Incident Response Plan (CIRP):

The Election Commission will implement and regularly review a comprehensive Cyber Incident Response Plan (CIRP). This plan will include clear procedures for identifying, containing, eradicating, and recovering from cyberattacks specifically tailored to address threats outlined in the methodology and the 70 questions.

9.2 Incident Response Team Practice:

The core and extended incident response teams will practice their response capabilities at least annually using tabletop or functional cybersecurity exercises. These exercises will simulate scenarios based on the identified threats, ensuring that the teams are well-prepared to respond effectively to real-world cyberattacks.

10. Inventory Management:

10.1 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.

10.2 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.

11. Data Management Practices:

11.1 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.

11.2 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.

12. Software Development Security:

12.1 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.

12.2 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.

13. Mobile Device Management:

13.1 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.

13.2 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.