Election Data Integrity and Data Transfer Security

A PRACTICAL FRAMEWORK

ELECTION SECURITY *Exchange*

> Election data integrity ensures that critical election information, from voter records to tabulation data, remains intact and free from unauthorized modification throughout the election lifecycle. These practices ensure elections are secure, accurate, transparent, and trustworthy.

Data integrity includes protecting data at rest (information that is stored and not actively moving), or information that is stored physically (e.g., paper voter registration records, paper ballots, etc.) and digitally (e.g., on a server, computer, external media, etc.), as well as data in transit (i.e., moving across the internet, between systems, etc.). There are different approaches and methods for protecting each type, as well as for data at rest versus data in transit. This guide introduces a framework to help election offices identify, manage, and validate their data, procedures, and systems.

Protecting the integrity of election data is not just a technical task; it is a core election security function. Every safeguard that preserves the accuracy and consistency of voter records, ballots, tabulation data, etc., also strengthens the overall security posture of an election office. When data is well-governed, well-protected, and routinely verified, it becomes harder for errors, disruptions, or malicious activity to undermine operations or public confidence. This is why data integrity practices sit at the center of election security, providing the structure that supports resilience, transparency, and trust throughout each election cycle.

Core Foundation of Election Data Integrity

Establish clear governance, professional training, and compliance with elections laws. You can accomplish this by:

1. **Identifying Critical Data:** Qualify data by its criticality and importance to the conduct of the election.
2. **Protecting the Data:** Place the necessary security measures on the data, systems, and physical locations where the data is stored.
3. **Verifying the Data:** Ensure data on different systems or used in different processes are identical and have not been altered.
4. **Maintaining Resiliency:** Maintain recovery and continuity capabilities.

People & Governance

Data integrity is only as strong as the organizational culture. This foundation ensures that every process is backed by standardized procedures, comprehensive staff training, strict adherence to election laws, and continuous monitoring and auditing.

Key Practices

- Standardize and document procedures
- Define roles and accountability
- Provide thorough and regular staff training
- Ensure legal compliance
- Continuously monitor and audit the steps above and the data itself

1. Identify Critical Data

Election data must be accurate, complete, consistent, and reliable across all systems, including voter registration, ballot definition, and results reporting. Errors introduced early in the process can carry through to final results, making data quality a foundational security requirement for integrity.

For example, voter registration data can come from multiple sources, including paper registrations, online registrations, third-party registration entities accessing online registration, motor vehicle systems, etc. Each of these inputs can result in data not coming across correctly to the voter registration system. Paper registrations may be incorrectly typed by staff, and external sources such as motor vehicles and third-party registration entities may send data that is not supposed to be sent, or vice versa. Procedures for ensuring data accuracy and integrity across these systems tend to be well known and continuously monitored. But what about other source data, such as mapping systems or GIS systems, which are inputs to a voter registration system to ensure a voter gets placed in the correct districts and precincts. Furthermore, that district data is an input to the voting system, which ensures candidates and contests get assigned to the correct ballot style(s). Similarly, candidate and contest data may be imported from a candidate filing system that accepts manually entered data from paper filings and online filings.

Mapping the data lifecycle to its origin and validating the data at the point of input, or original receipt of the data (in the case of online data input by another party), will minimize the likelihood that incorrect information flows from system to system. Additionally, tracking the data informs election officials about which systems the data resides in.

Key practices:

- Assess and document what data is most critical to track
- Identify the original source of data
- Map the locations or systems where the data resides

2. Protect Election Data

Election data must be protected from unauthorized access or modification through strong controls and secure processes, including defense-in-depth measures. Protective measures mitigate the risk of unauthorized access and modification, ensuring data integrity.

Protective measures alone are not enough. Election offices must also put detective measures in place, such as ongoing monitoring and auditing that identifies when data was accessed and flag unauthorized or unexpected changes before they affect operations.

Key practices:

- Control physical access to equipment
- Implement role-based access controls (i.e., only allow employees to access data they need to perform their job duties)
- Ensure two-person and bipartisan rules where applicable
- Implement detective measures, such as tamper-evident seals, alarms, security cameras (e.g., CCTV), etc.
- Log all changes to critical data
- Encrypt and digitally sign critical data
- Create and store a hash of critical electronic data, especially before transferring it to another system (a hash is a digital fingerprint of a file that changes if even one character is altered, making it easy to verify the file arrived intact)
- Create encrypted backups and store them in a secure location offline and away from the original source

Data Transfer and Interoperability

Election offices routinely interface with local government systems, state agencies, and, in some cases, federal systems. These interactions require a multi-layered approach to data transfer security that blends industry standards, federal requirements, and state-specific statutes. Because many data exchange protocols are defined outside the election office, jurisdictions must operate within externally established frameworks while ensuring secure implementation at the local level.

To ensure data is not unintentionally or intentionally modified during the data transfer process, election officials should protect and validate the integrity of the data at the time of export and again once imported into a new technology. Election technologies and systems store data in different formats, so it is imperative that the data be validated or verified once it moves from one system to another.

Key practices:

- **Internal Data Transfer**
  - » Use secure, controlled methods for moving data within election systems. This may include physical air-gapping, where ballot programming from EMS is transferred to tabulation systems and results are transferred from scanners to tabulation systems using encrypted, write-once media (e.g., USB devices), with strict chain-of-custody procedures.
  - » Encrypt and hash to protect and ensure integrity or use digital signatures for both protecting and ensuring data integrity.

- **External Data Transfer**
  - » Data exchanges with outside entities (e.g., the Secretary of State, DMV, Social Security Administration, Vital Statistics Offices) may be subject to federal requirements and will generally also be required to comply with state-specific laws, rules, and protocols. In addition to the "Internal Data Transfer" practices noted above, additional practices may include secure web services, SFTP transfers, or API-based integrations.
  - » Audit the data once received. If the source file does not include integrity checks, such as hash validation or digital signatures, request information or reports that allow you to verify that the exported data matches what was received or imported. Produce similar information or reports for data you export and provide the information to the applicable outside entities so they can verify what they receive.

3. Verifying Access and Integrity of Election Data

Recognizing that data has been accessed or modified requires continuous monitoring and auditing the data. Many of the protective measures above only hinder the ability to access a system, but in order to ensure that no one has accessed or incorrectly modified it you must detect that the changes occurred. Ongoing monitoring that includes reviewing log data, chain of custody records, verifying data across systems or paper records, and anomaly detection is essential.

Key practices:

- Assess audit log data for anomalies
- Validate digital records against the source record, including paper records where applicable
- Use tools to identify anomalies, like VoteShield[1] for voter registration records
- Use a Security Information and Event Management (SIEM) system to aggregate and review log data, etc. (Software that collects logs from systems and alerts you to unusual patterns)
- Provide transparency and allow public observation, and where anomalies are identified, review or investigate the data.

1 https://www.voteshield.us/

4. Maintain Recovery and Resilience

When a data integrity issue is detected, the election process must include mechanisms to recover from errors, restore data to a trusted state, and continue operations during and after the anomalous activity. This includes reverting to backup sources of the data, redundant systems containing the data (e.g., the original source), paper copies, etc. To ensure the backup copies or alternate sources are reliable, ensure the recovery procedures are documented and tested, and that all staff have been trained on continuity of operations procedures, as it will likely take your entire team working in parallel to restore normal operations.

Key practices:

- Maintain regular system backups of all critical election data, stored offline and separate from the original source when possible
- Test data recovery procedures regularly
- Develop continuity plans
- Prepare for system failures or disruptions

Citations

1 **U.S. Election Assistance Commission, Election Security Resource Library**
https://www.eac.gov/sites/default/files/electionofficials/security/Best_Practices_for_Election_Technology_508.pdf
Voluntary Voting System Guidelines (VVSG 2.0)
https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines

2 **Salesforce, What is Data Integrity**
https://www.salesforce.com/data/what-is-data-integrity

3 **IBM, Data Integrity Overview**
https://www.ibm.com/think/topics/data-integrity

4 **National Institute of Standards and Technology (NIST).**
Election Security Series: Data Integrity and Recovery
https://www.nist.gov/system/files/documents/2023/01/06/DataIntegrity-ElectionSecurityGuide-Factsheet.pdf
NIST SP 800-52 (TLS Guidelines)
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf

5 **Brennan Center for Justice, Access to Election Data and Equipment**
https://www.brennancenter.org/our-work/research-reports/requests-access-election-data-and-equipment-require-balancing-risks-and

6 https://www.cisecurity.org/services/albert-network-monitoring
https://www.ignet.gov/sites/default/files/files/Best-Practices-for-Federal-Agencies-to-Strengthen-Cloud-Security.pdf
https://www.nist.gov/system/files/documents/itl/vote/draft-_nistir_7711_june2010.pdf