Rapid Election Data Backup and Verification

PDF

Download this guide as a PDF, to read offline or to attach to an email.

Purpose

This guide provides practical procedures for creating rapid, secure backups of election data as it becomes available during normal election workflows.

The objective is to ensure that critical election records remain available for independent verification, audit and analysis, disaster recovery, and continuity of operations. This is particularly important in situations where physical records or systems are removed from custody, data systems become unavailable, or records are lost due to natural disaster or system failure.

Core Principles

Backups should be created as soon as data becomes available and should include all relevant data types, not just ballot images. Each backup should be duplicated so that at least two independent copies exist in separate locations. All backups should be accompanied by cryptographic hash values so their integrity can be verified. Once exported, backup data should not be modified.

Caveat

Although we are generally familiar with voting system software and how ballot images and CVRs can be exported (see Exporting Guide, the procedures described here serve a different purpose. The goal is to produce rapid, interim backups during the election process so that an unexpected interruption does not result in a substantial loss of data.

Election management systems are not typically designed to support comprehensive exports during active election operations. As a result, the availability of data may be limited or incomplete at any given point in time. For example, full Cast Vote Record (CVR) datasets are often not finalized or exportable until processing is complete. Similarly, logs, adjudication records, or consolidated

reports may only become available at later stages. However, other files may be available that are not in final reported form that may still help in a loss situation.

Accordingly, these backup procedures should be understood as capturing the maximum available data at each point in time, rather than producing a complete or final dataset. Incremental or partial exports are still valuable, particularly for preserving ballot images and intermediate records that may not be reproducible if lost.

Jurisdictions should work within the capabilities of their systems to perform exports as early and as frequently as practical, recognizing that some data elements will only be available after the election has concluded.

Please share any limitations encountered with these procedures with our team at info@auditengine.org so that guidance can be refined over time.

When to Perform Backups

Polling Place Scanning

After scanners are closed, ballot image data and CVRs should be transferred to the EMS. A snapshot backup should then be created that captures all ballot images and any associated data available at that time. This process should be repeated after all polling place uploads are completed.

Typical checkpoints include the end of early voting and the completion of election day uploads.

Central Scanning (Mail / Provisional Ballots)

At the end of each processing day, newly scanned ballot images and any updated CVR data should be exported. A snapshot backup should then be created reflecting the cumulative dataset available at that point.

Final Backup

After all processing is complete, a final export should be performed that includes all ballot images, final CVRs, logs, and reports. This serves as the definitive archival copy.

Data to Include

Each backup should include, when available:

- ballot images in the format generated by the system, such as PDF, TIFF, PNG, etc.
- cast vote records (CVRs), whether partial or complete
- election definition files
- batch and precinct reports
- system and adjudication logs
- adjudication records
- e-pollbook data
- any other data normally generated by the system, such as any reports.

Backup Procedure

Data should be exported directly from the EMS or central tabulation system using the system's standard export functions. Files should not be filtered, modified, or reorganized, and the original directory structure should be preserved.

The exported data should be exported to at least two separate storage devices. These may include encrypted USB drives, solid-state drives, or secure network storage. Each copy should be treated as independent and complete.

Each copy should be stored in a separate secure location, preferably in different government facilities. This separation provides protection against physical loss, localized damage, or investigative seizure affecting a single location. When available, store backup media in a locked safe, secure storage room, or access-controlled cage within a monitored facility.

Hash Generation and Verification

Cryptographic hashes provide a reliable method for confirming that files have not been altered. Publishing hash values does not reveal the contents of the data and allows independent verification by third parties.

SHA-256 is the recommended standard.

To generate hashes on Linux or macOS systems, assuming all files are in a single folder. `cd` to that folder, then:

```
sha256sum * > sha256_manifest.txt
```

On Windows PowerShell, use:

```
GGet-FileHash -Algorithm SHA256 * | ForEach-Object { "$($_.Hash)  $($_.Path)" } |
Out-File sha256_manifest.txt
```

The commands above should work on the system that you use to create the data for the thumbdrives without adding any other data.

For windows, consider using the sha256sum utility, same as on Linux. In many windows systems, this is already installed. If not, you may consider installing.

1. Install Cygwin
2. visit: https://www.cygwin.com/install.html
3. You need to select and download `setup-x86_64.exe` typically for windows machines.
4. Run installer with this command at a command prompt `setup-x86_64.exe -q -P coreutils`
5. Add the c:\cygwin64\bin folder to the PATH so this command is available in a cmd terminal (there are also other methods):

   setx PATH "%PATH%;C:\cygwin64\bin"
6. Open a cmd terminal and check it with `sha256sum --version`
7. Go to the folder that contains the files for the hash manifest, and use:

   sha256sum * > sha256_manifest.txt

To verify hashes on a separate system:

```
sha256sum -c sha256_manifest.txt
```

All files should report as OK. You can also manually check the hash for any specific file by creating the hash:

```
sha256sum filename
```

Publishing Hash Values

Election offices are encouraged to publish the hash manifest along with total file counts and total data size. This information may be posted on an official website, included in a public records portal, or released through a formal public notice.

Publishing this information allows independent validation of data integrity and strengthens public confidence in the preservation of election records.

Chain of Custody Considerations

The time and method of each export should be documented, along with the personnel involved. Storage locations for each copy should be recorded, and any transfers or access should be logged.

Risks of Not Performing Rapid Backup

If backups are not performed promptly, original data may be altered during adjudication, overwritten, or lost. Logs may be truncated, and it may become difficult or impossible to reconstruct a reliable record of the election.

Relationship to Data Submission

For guidance on submitting data for independent audit, see Sending Election Data to AuditEngine.

Summary

Rapid, verified backups are a low-cost safeguard that preserves election data integrity, supports independent verification, and ensures continuity under adverse conditions. These practices can be implemented within existing workflows with minimal disruption.