

Welcome — A Plan for Provable Elections

An implementation guide for the people who will run it

A welcome from the work ahead

Thank you for considering this work. Election offices already carry the responsibility of protecting a process that neighbors, families, and future voters depend on. You are not being asked to fix a failure of effort. You are being invited to help close a gap in the record: the lack of custody evidence that an outside person can independently check.

StrongRoom is designed to add evidence without adding authority to software, taking authority away from your office, or changing how votes are counted. Your procedures, certified systems, and named decision-makers remain in charge. The purpose is simple: make the care your team already brings to elections easier to demonstrate later.

The promise in one sentence

This is a way to prove a process, not a replacement for the process.

What this changes for you, day to day

You will work from one custody record, presented through six controlled views: poll workers, jurisdiction command, security, legal, audit, and review. Each view is limited to the role and authority of the person using it, while the underlying record stays consistent.

For your team, that means a clearer place to record administrative custody events for physical mail-ballot packages, incidents, equipment movement, and access to secured areas. Instead of assembling the story later from binders, spreadsheets, transfer forms, email threads, and memory, you have evidence that can be checked against the sealed history.

Human authority stays with you

Every consequential action requires named human approval. Software never approves, rejects, or certifies anything on its own.

What it will never do

The boundary matters. StrongRoom is not a voting system, a tabulator, or an authority over a ballot. Paper stays authoritative.

No. It does not mark ballots.

No. It does not tabulate votes or report results.

No. It does not decide voter eligibility.

No. It does not replace certified voting systems.

No. It never decides whether a ballot is valid.

The work begins and remains focused on evidence for administrative custody. Established voting, tabulation, certification, and audit systems keep their own roles.

How the proof works, in plain language

The system uses ordinary ideas with strict discipline: write down what happened, seal the history, and make it possible for someone else to check whether the history has been changed. Four safeguards work together.

1. An append-only history

Events are added to the record; earlier events are not quietly rewritten, removed, or reordered. When the history is sealed, an alteration becomes visible rather than invisible.

2. Independent outside witnesses

Outside witnesses counter-sign the sealed state. That makes it harder for anyone to present one version of history to an auditor and a different version to the public. If the witness condition is stale, suspended, undersized, or conflicted, the system treats that as a refusal to proceed, not a warning to ignore.

3. Sealing authority is shared

The power to seal the record is split across multiple guardians so it does not rest with one person, one server, or one vendor.

4. Two people on sensitive steps

Sensitive steps, including batch sealing at envelope separation, require two distinct officers. The required dual control is part of the evidence, not only a rule in a manual.

Voter privacy is protected by design, not by discipline

The identifier in this system belongs to envelope custody, not to a vote. It never encodes selections.

After an envelope is separated from its ballot, no key, token, reused identifier, foreign reference, or query path is allowed to reconnect a voter to ballot content. This is not a promise that staff must remember to keep. The boundary lives in the data model itself.

Public evidence is designed to be checkable without disclosing more than it should. Precise separation times are suppressed, membership lists are replaced with commitments, and published records can still carry a digest and signature that can be recomputed from the information disclosed. Privacy is considered across the whole set of records, including linkage, ordering, timing, small-group disclosure, and combinations of otherwise safe outputs.

A practical privacy promise

Your team should never have to choose between proving custody and protecting the secret ballot. The system is built to hold both boundaries at once.

The plan we are following

Start in shadow mode

The first step is a shadow pilot in a single jurisdiction, alongside existing systems. Nothing is binding. The focus is custody evidence first: incident reporting, equipment tracking, ballot custody, evidence logs, procedures, and access controls.

Review before expansion

Independent cryptographic and legal review is a gate, not a formality. Only after that review and an end-to-end pilot can expansion be considered.

Keep sensitive evidence local

Deployment is local-first. Sensitive evidence remains inside the authorized boundary instead of being pooled for routine use elsewhere. Work is separated into three isolation tiers: public-facing services, election-data processing, and tightly controlled sealing infrastructure.

The implementation posture

Build carefully, test in the real procedures you already use, refuse weaker modes rather than silently falling back, and preserve evidence of each release and decision.

What we ask of you, and what you can expect from us

A good pilot is a working partnership. You know your people, procedures, authorities, and local realities. We bring an evidence system that must earn its place in that work.

What we ask of you

A shadow environment. Let the custody evidence operate beside your existing systems, with no binding role.

Procedural feedback. Tell us where the workflow helps, where it slows you down, and what your local rules require.

Honest criticism. Raise concerns early. A trustworthy record begins with a system willing to hear what is not working.

What you can expect from us

No binding role. The pilot will not approve, reject, certify, mark, count, or report anything.

Published limits and no surprises. We will state what the system can and cannot do, and surface refusal conditions instead of hiding them.

Training and documentation. Your team will receive clear, role-aware guidance before work begins and support as procedures are tested.

A simple way to begin

Start with one shadow environment and one familiar workflow. Identify the people who should see each controlled view, walk through the procedure together, and record what needs to fit your office better. The first goal is not to change everything. It is to learn, safely, whether the evidence is clear, usable, and faithful to the work being done.

Your experience is part of the design

Poll workers, clerks, elections IT staff, security officers, legal and audit teams, and partner organizations each see a different part of the day. The implementation becomes more trustworthy when those perspectives shape it early.

Your authority remains visible throughout. The system records approvals; it does not create them. It records procedures; it does not overrule them. If a safety or evidence condition is not met, the honest outcome is a clear refusal and a record of why, never a quiet workaround.

Where we are honest with you

A system whose whole value is honest evidence cannot afford to overstate itself. These are the limits we state plainly, so your team can judge the work with clear eyes.

Not federally certified

StrongRoom is not EAC-certified under VVSG 2.0 and is not offered as a system of record for a binding election.

Demonstrations use synthetic data

Public proof runs use synthetic data. Real scan-event ingestion depends on authorized postal tracking access, which is still a gate.

Independent review is still outstanding

Independent cryptographic and legal review is not yet complete. That review is a required gate before expansion.

Guardian independence is not yet physical

Multiple guardians can currently be simulated on shared infrastructure. Until guardians operate on genuinely independent infrastructure, that control does not fully protect against the operator.

Residual risks are documented rather than hidden

The documented risks include colluding officers, guardian collusion, print-vendor token access, limited coercion resistance, and dependence on verifier implementations. Cryptography narrows institutional trust; it does not eliminate it.

An invitation to build the next careful step

If this approach fits your office, we invite you to help test it in the open and practical spirit it requires. Bring your procedures, questions, objections, and standards. Together, we can upgrade election technology responsibly while keeping the authority of people, paper, and law where it belongs.

The goal is not a perfect promise. It is a more provable process, built with the people who run elections and worthy of the children who will inherit the trust we leave behind.