NXT ASSETS

Introductory Concepts

For Election Administrators and Warehouse Managers

Next Election Services, LLC | April 2026

Introduction

A single voting machine moves through a warehouse, onto a truck, into a polling place, back into custody after the polls close — and every one of those movements has to be documented, signed, and provable months later.

Elections are unforgiving. One missing ballot box, one undocumented seal break, one unexplained gap in the custody record, and an administrator is answering questions to the Secretary of State, to a county attorney, or to a courtroom. The stakes are not abstract — they are written into state statute and federal law, with retention periods measured in years and criminal penalties for destruction of records.

NxtAssets is the system election offices use to keep every piece of equipment, every box of ballots, every seal, and every handoff accounted for — from the shelf in the warehouse to the polling place and back. This document introduces the six concepts that shape how the platform works in practice.

What this document covers

- **Chain of custody.** Who handled what, when, and where — signed, timestamped, and impossible to rewrite.
- **Operational visibility.** Knowing what every asset is and where it is, in real time, across GPS, Bluetooth, RFID, and whatever identifiers the county already uses.
- **Work orders and workflows.** The plan-and-execute layer that turns election prep into tracked, assigned, step-by-step tasks.
- **Seal management.** Every required seal applied, inspected, and logged — with broken seals surfaced immediately.
- **Asset nesting and kits.** Cases inside pallets, devices inside cases, ADA components inside polling-place kits — handled in groups without losing individual tracking.
- **Audit trails and accountability.** The permanent record of everything the system observed, tamper-evident and ready for oversight.

Chain of Custody

A *chain of custody* is the documented trail that shows who handled an asset, when, and where. In elections, it is the difference between "we think the ballot box was sealed" and proof that it was — signed, timestamped, geolocated, and impossible to rewrite later.

Why it matters

A voting machine travels from Warehouse A to a truck, to Precinct 12, sits for a day, then travels back. Half a dozen people touch it along the way. If any one of those handoffs is not documented — and a seal later turns up broken — no one knows who to ask. That is the failure mode chain of custody is designed to prevent.

The requirement is not optional. Texas Election Code §129.051(b) requires two or more individuals at every custody transfer of electronic information storage media. The federal Election Assistance Commission's 2021 *Chain of Custody Best Practices* raises the floor: at least two signatures on every transfer record, with a detailed description of the item, seal numbers, party names, date, time, and location. NxtAssets enforces both, because the work order does not advance until the record is captured.

What every handoff captures

When an asset changes hands or locations, NxtAssets prompts for a handoff record. The record contains:

- **Parties involved.** Who released the asset and who received it — names and IDs on both sides. A warehouse manager handing off to a transport driver. A polling-place judge receiving a sealed voting machine from a delivery team.
- **Digital signatures.** Collected on a mobile device or tablet. Each person signs directly in the NxtAssets app to certify the handoff.
- **Date and time.** Automatic, to the second.
- **Location.** GPS coordinates when the device has them; otherwise the known site — "Warehouse A" or "Precinct 12."
- **Event type.** "Assigned to Polling Place 12." "Handoff to Poll Worker." "Returned to Warehouse." Context, not just coordinates.
- **Additional notes.** Seal numbers, equipment condition, anything the workflow requires at this step.

Why the record cannot be rewritten

Every custody event is written to a **write-once log**. Once the record is in, the system refuses to change it or remove it. That rule is enforced below the application — not by a policy someone can override, but by the way the data layer is physically built. Nobody can quietly edit last month's handoff.

Retention is set to match statute. Precinct records under TEC §66.058 are preserved for 22 months; electronic-storage-media records under TEC §129.024(b) carry the same 22-month floor. The retention window can be made longer by configuration; it cannot be shortened to drop records before their time.

> **In practice. At 9:47 a.m. on election day, Precinct 12 calls Warehouse A: one of the voting machines has a broken seal on the memory-card door. The election director opens the machine's custody record in NxtAssets. The last four handoffs — name, signature, timestamp, GPS coordinates — scroll by in seconds, alongside the seal event log showing when the seal was applied, by whom, and its inspection history. The machine was last handed off to a poll worker at 6:42 a.m.; the seal was intact at that point. Whatever happened, happened in the hour after the polls opened, at Precinct 12. The investigation has a starting point, and it has it inside of a minute — not a week.**

Workflow integration

Chain-of-custody checkpoints don't live alongside the workflow. They *are* the workflow. Default NxtAssets workflows build handoff events into each statutory transition: Truck Loading, Equipment Drop-off, Judge Handoff, Rally Point Drop-off. Staff cannot skip them, because the work order will not mark the step complete without the signature.

If a jurisdiction has its own procedure — a witness signature the state does not require but the county prefers, an extra approval step — the workflow is extended through configuration. No code changes.

Operational benefits

- **Audit response.** When the Secretary of State asks for custody records, the office exports them — it does not reconstruct them.
- **Public records requests.** A FOIA-style request for chain of custody is a report run, not a hunt through binders.
- **Accountability at every touchpoint.** Every person who handles an asset knows their name is on the record. That deterrence is as valuable as the record itself.
- **Post-election review.** Custody timelines support after-action reports and next-cycle planning — which routes were slow, which handoffs were contested, which procedures need revision.

Operational Visibility

On election day there is no substitute for knowing where every asset is, right now. NxtAssets combines three tracking technologies and a unified identifier model into one live picture — so a warehouse manager, an election director, and a field tech are all looking at the same map, reading the same inventory, and finding the same machine whether they scan a barcode or read an RFID tag.

Why it matters

Election day produces a continuous stream of small questions. Are the voting machines en route to their polling sites? Did the supply boxes reach the right locations? Is any truck delayed or off-course? A single voting machine may carry a manufacturer serial number, a county asset tag, an RFID label, and a Bluetooth beacon — all of them referring to the same physical unit. The team that can answer "where is this, and are we sure it's the right one" in seconds is the team that solves problems before they become incidents.

Three tracking technologies, one picture

Different parts of the election cycle need different kinds of visibility. NxtAssets does not force one answer on every problem — it uses the right tool at each stage.

- **GPS — wide-area, in motion.** Cellular GPS units on delivery vehicles and high-value cases broadcast live location. Useful for knowing a truck full of equipment is on its planned route, or noticing that a delivery is running late before the polling place calls to ask.
- **BLE — indoor, at rest.** Bluetooth Low Energy beacons attach to individual assets or containers. A mesh of BLE beacons and Wi-Fi access points in the warehouse pinpoints equipment to the shelf. In the field, a tablet senses when a specific asset has entered a specific room or zone.
- **RFID — bulk and checkpoint.** RFID tags (passive or active) are scanned at loading docks, polling-place entry points, and return stations. Useful for fast bulk scans — a pallet of equipment passing a reader in seconds — and for enforcing checkpoint-based workflow transitions.

Many identifiers, one asset record

Traditional inventory systems tag an asset with a single ID. Election equipment does not work that way. A voting machine carries the manufacturer's serial, the county's asset-tag barcode, an affixed RFID tag, sometimes a BLE beacon, sometimes a GPS tracker ID — and staff in the field may know it by the sticker number that went on it in 2019.

NxtAssets stores all of those identifiers against the same asset record. The supported identifier types are:

- **Serial number** — the manufacturer's unique code on the device.
- **Asset-tag barcode or QR** — the county's own internal inventory label.
- **RFID tag** — passive UID stored for short-range scanning.
- **Bluetooth beacon ID** — UUID or major/minor for indoor tracking.
- **GPS tracker ID** — the SIM or device ID of an attached tracker.
- **Other codes** — license plates for vehicles, MAC addresses for networked gear, legacy IDs from prior systems.

In practice, this means a technician in the field can scan a QR code on a voting machine to pull it up in NxtAssets, while a warehouse antenna reads the RFID tag on that same machine as it rolls out the door. Both actions tie back to the same record. The system knows all those IDs belong to one item.

The multi-identifier model also protects against scanning errors. At intake, a worker might scan *both* the barcode and the RFID of a machine — if the two don't resolve to the same record, something is wrong and the system flags it before the mistake propagates.

The live picture

Open the NxtAssets dashboard and you see a live map. Trucks move along their delivery routes as icons. Each tracked asset shows its last known position. On election morning, a warehouse manager watches outgoing deliveries; at the same time, an election director monitors which polling places have received equipment and which are still waiting. When a site is running behind, it is flagged immediately — the response is a phone call, not a search.

Location history is logged automatically. Every scan and every tracker ping is written with its timestamp, so after an election a machine's trail reads like a diary: *delivered to Site A at 6:45 a.m. by Truck 3, moved to Room 101 at 7:00 a.m., picked up at 8:15 p.m., returned to Warehouse at 9:00 p.m.* That timeline is the *where* counterpart to the chain-of-custody *who* — automatic, and evidentiary.

> **In practice. Election morning, 5:30 a.m. The election director opens the live map in NxtAssets from her desk at Warehouse A. Twelve delivery routes are in progress; ten are on schedule, one is ahead, one is ten minutes late because of an accident on the highway. She watches that truck reroute automatically on the map, with the updated ETA flowing to the polling places waiting for it. At the same time, a warehouse tech scans a pallet leaving the loading dock. The RFID reader logs nine voting machines, four ballot scanners, and two ADA booths — the pallet's expected contents — in under four seconds. The manifest ticks green. Nothing has to be**

> **re-scanned, nothing has to be called in, nothing has to be written down.**

Geo-fences and alerts

Draw a virtual boundary around a polling place, a warehouse, or a planned delivery corridor. If a tracker crosses the wrong line — a truck leaves its route, a ballot container exits secure storage outside working hours — NxtAssets fires an alert to designated personnel in real time. Proactive monitoring, not post-hoc forensics.

Operational benefits

- **Continuous awareness on election day.** No frantic phone calls to locate a missing voting machine; no wondering whether all sites opened on time.
- **Faster problem resolution.** Breakdowns, wrong-site drops, late arrivals — identified and acted on while there is still time.
- **Automatic** *where*. The location history complements chain-of-custody records without requiring anyone to write anything down.
- **Continuous inventory.** The system knows which assets are in which location without a manual count.
- **Route analysis for next cycle.** Which routes took longer than planned, where bottlenecks formed, what to change before the next election.

Work Orders and Workflows

A Work Order is the system's version of a job ticket — who does what, to which assets, by when. A Workflow is the path the ticket follows, step by step, with enforcement. Together they turn election prep from a spreadsheet-and-memory operation into a tracked, assigned, auditable process.

Why it matters

An election is thousands of tasks running in parallel. Voting machines have to be unboxed, firmware-updated, tested, cleaned, sealed, and packed. Polling-place kits have to be assembled to the right specification. Trucks have to be loaded in the right order. Supplies have to be returned, reconciled, and stored. One missed step — a memory-card seal that never got applied — can cost an election office a week of investigation and a hit to public trust.

Work orders and workflows are the mechanism that makes sure steps aren't missed. Every task is owned by someone. Every action is time- and user-stamped. Every checklist has to be completed before the work order marks itself done.

What a Work Order is

A Work Order in NxtAssets is a structured job assignment. It defines what needs to be done, to which assets, at which location, by when, and by whom. Typical examples:

- **Prepare voting machines for the upcoming election** — firmware update, logic-and-accuracy test, cleaning, sealing.
- **Pack the Precinct 12 polling-place kit** — ballots, forms, signs, ADA equipment, supply box.
- **Deliver election-day equipment to Precinct 12** — 10 voting machines, 5 ballot scanners, 2 ADA booths, 12 supply boxes. Each physical unit is linked to the work order by serial number.
- **Service a malfunctioning ballot scanner** — bring in, diagnose, repair, re-test, re-seal.
- **Conduct a pre-election inventory audit** — walk the warehouse, scan, reconcile against the central registry.

When staff execute the work order, they use the web or mobile app to update it as they go. A team loading a truck opens the "Precinct 12 Delivery" work order, scans each item's barcode or RFID, and the system shows progress in real time — *10 of 10 voting machines loaded, 5 of 5 ballot scanners loaded.* When the truck leaves, the order goes to *In Transit*. At the destination, the receiving party scans items as they arrive,

confirming delivery against the same manifest.

Checklists that enforce order

Each work order can carry a checklist of steps that must be completed in sequence. A "Prepare Voting Machine for Deployment" checklist, for example, might run:

- Perform diagnostic test.
- Clean the scanner.
- Install tamper seal on memory card slot.
- Record seal serial number in the system.
- Pack machine in its case.

The system can enforce the sequence. If a step is skipped, the work order stays incomplete and surfaces to the supervisor as a red flag. This is how the platform prevents a voting machine from arriving at a polling place without its seal: the task is not allowed to finish until the seal is recorded.

Real-time work-order status

Dashboards show every work order's status — *Open, In Progress, Completed* — by election, by location, by task category. As election day approaches, a manager can see that ninety-five percent of ballot scanners have passed logic-and-accuracy testing, that three polling-place kits are still being packed, and that two delivery work orders are behind schedule. Reallocation is a decision, not a discovery.

What a Workflow is

A Workflow defines the broader path a work order follows — the sequence of states, the rules governing each transition, the roles permitted to move things from one state to the next. The NxtAssets workflow engine is a state machine: every process (*Deliver Equipment to Polling Site*, *Conduct Logic and Accuracy Testing*, *Close Polling Place*) is modeled as a series of states and the allowed transitions between them.

A simplified "Deliver Equipment" workflow moves through *Ready for Delivery* → *In Transit* → *Delivered* → *Confirmed Received*. The system enforces the actions required to move from state to state — scanning all items and capturing a chain-of-custody signature is what transitions a delivery from *In Transit* to *Delivered*.

Configurable without code

No two jurisdictions run elections exactly the same way. Workflows are configurable through an administrative interface — not through programming. The platform ships with preloaded, best-practice election workflows that include chain-of-custody checkpoints and seal checks by default. When a county has its own procedure (an extra witness signature, a supervisor-approval step for certain transfers, a Post-Election Audit Inventory sequence that doesn't exist elsewhere), an administrator adds the step through configuration. No code changes, no vendor release cycle.

Role permissions are part of the configuration. Only the *Warehouse Manager* role can mark a work order "Packed"; only the *Polling Place Judge* role can mark it "Received." The rules are enforced at the state-transition level so the right people do the right actions at the right time.

> **In practice. Two weeks before the general election, a new Secretary of State advisory introduces a mandatory supervisor-approval step before voting equipment leaves the warehouse. The county's IT director opens the "Dispatch Equipment" workflow editor and inserts a** *Supervisor Approval* **state between** *Packed* **and** *Ready for Delivery***. The step requires a named supervisor's login to advance. From that afternoon forward, no delivery work order can move past** *Packed* **without that sign-off. No code was written. No vendor ticket was filed. The change was live before the 5 p.m. staff meeting.**

Operational benefits

- **Adaptability.** When laws change or local practice evolves, the system changes with it. Configuration, not procurement.
- **Consistency.** Workflows are a standard operating procedure embedded in software. Every staff member follows the same steps in the same order.
- **Compliance.** Statutory sequences can be enforced — if the law says step X must precede step Y, the system does not allow Y until X is done.
- **Transparency.** At any point, a manager can see which tasks are in which state and who is responsible for each.
- **Accountability.** Every work-order action is time-and-user-stamped. If a step was skipped, the system knows who skipped it.

Seal Management

Tamper-evident seals are how an election office proves equipment stayed untouched between the moment it was prepared and the moment it was used. Managing which seal is on which device, at which seal point, and whether every seal is still intact — on paper, that is a job no warehouse ever gets completely right. NxtAssets makes it an automated part of the asset record.

Why it matters

A ballot scanner may have three required seal points — one on the memory-card door, one on the access panel, one on the transport-case latch. A ballot box has a slot seal and a lock seal. A provisional-ballot bag gets sealed at the polling place, opened at the counting center, resealed. Multiply by hundreds of devices, across dozens of polling places, across a prep cycle that runs for weeks, and the scope of the paper problem becomes obvious.

NxtAssets treats seals as their own class of tracked items. Each seal has a unique serial number; each seal type (red zip-tie, cable lock, tamper-evident sticker, padlock) is defined in the system; each seal *point* on each asset type is defined too. The system knows that a ballot scanner should have three seals applied before it leaves the warehouse. If one is missing when the work order tries to close, the task does not finish.

How the lifecycle is tracked

Each seal event is a logged, time-stamped, attributed record.

- **Application.** When a seal is applied to an asset, a staff member scans the seal's barcode or ID and associates it with the asset and the specific seal point. The record captures which seal, to which asset, at which point, when, and by whom. Example: *Seal #A123456 (red zip-tie) applied to Scanner Unit #5 — memory-card slot — on Oct 30 by Tech John Smith.*
- **Inspection.** During seal audits, a poll worker or roving technician scans the asset, pulls up the expected seals by serial number and position, inspects the physical seals, and logs *audit pass* or *audit fail* with a timestamp. Failed audits trigger immediate alerts to administrators.
- **Removal.** Seals are removed only at authorized times (at the end of voting, during post-election processing, to service a malfunction). Each removal is logged as a Seal Event with the reason, the user, and the timestamp.
- **Replacement.** If a seal must be broken to address an issue, a new seal is applied and tracked the same way. The chain is never broken silently — only deliberately, and only with a record.

Workflow-enforced seal checks

Seal policies are not advisory. They are steps inside the workflows that govern each phase of the election cycle. A "Close Polling Place" work order requires the poll worker to apply a seal to the ballot box and record the seal number before the task can complete. A "Dispatch Equipment" workflow does not move into *Ready for Delivery* until every required seal on every asset is recorded in the system. A missing seal at a required seal point is a flag, not a footnote.

> **In practice. Two weeks after the general election, an observer from a party organization requests proof that every voting machine had intact seals on election morning. The election director runs a single report in NxtAssets: for each voting machine, the machine's serial number, the applied seal numbers, the *audit pass* events logged by poll workers between 6:00 and 7:00 a.m., and the identity of the poll worker who performed each inspection. A thousand rows. Every row documented. The observer receives a CSV export by the end of the day, and the county commissioners receive a memo the next morning stating that every seal was verified intact before polls opened — with a verifiable log to back it up.**

Context-specific seal rules

Different assets and different contexts carry different seal rules, and NxtAssets configures accordingly.

- A **ballot box** requires a seal on its slot at close of polls. The system prompts the user closing the poll to apply it and record it.
- An **ePollbook case** may use two padlocks instead of disposable seals; padlock serial numbers are tracked the same way.
- **Provisional-ballot bags** follow a multi-step protocol — sealed at the polling place, opened at the counting center, resealed — and the workflow captures each seal check at each stage.

Operational benefits

- **Digital seal logs.** The paper seal log and its handwriting errors are gone. A scan captures serial, asset, point, time, and operator in one motion.
- **Mobile inspections.** Poll workers and roving techs perform seal audits on a tablet or phone; results are visible to supervisors in real time.
- **Deliberate exceptions.** When a seal must be broken to service a malfunction, the action is documented and a replacement is tracked. No silent breaks.
- **Seal-status reports on demand.** A manager can see which seals are applied, which have been replaced, and which require follow-up — without leaving the dashboard.

Asset Nesting and Kits

Election equipment rarely travels alone. A transport case holds a voting machine and its peripherals. A pallet holds cases. A polling-place kit holds everything a site needs for an election day. NxtAssets models these container relationships directly — and lets administrators define what every kit *should* contain for every kind of location and election.

Why it matters

A county's equipment is packed and shipped in groups. Scanning every single item at every handoff is slow, error-prone, and sometimes impossible — a sealed case is meant to stay sealed in transit. But losing sight of what is *inside* each container the moment you treat it as one unit defeats the point of tracking anything. Asset nesting gives operations staff the group-level handling they need without giving up the individual-level visibility they depend on.

How nesting works

In NxtAssets, any asset can serve as a container that holds other assets, and the hierarchy can go several levels deep. A transport case holds a voting machine, a barcode scanner, a headset, and power cables; the case sits on a pallet; the pallet loads onto a truck. Each relationship is a recorded link — the system knows every item on the truck because it knows every item in each case on each pallet.

Operations gain several advantages from this directly:

- **Streamlined check-in and check-out.** A sealed case containing a voting machine and its peripherals is scanned once at the handoff. All nested items are marked transferred in the same action.
- **Instant inventory of contents.** A help-desk query — *what is inside Container C-100?* — returns the answer from the asset record, not from someone's memory of what was packed.
- **Nesting history.** The system tracks not only current nesting but also how things were grouped over time. If a case was damaged, you can see which voting machine was inside it at that moment.
- **Loss prevention.** A missing container narrows the search to a known set of contents. A missing individual item points to the container it was last in — and that container's chain-of-custody record points to where it was handled.

Nesting is flexible. If a poll worker removes the voting machine from the case mid-day and later returns it separately, the system can record that un-nesting and re-nesting — the history reflects the actual movement.

Kits and the context-sensitive bill of materials

Not every polling place needs the same equipment. A large voting site may need extra booths. A location with accessibility requirements needs specific ADA components. An early-voting center needs more signage and extra ballot boxes to handle the volume. NxtAssets manages these variations through a **Product Configurator** that defines context-specific **Bills of Materials** — a BOM for every kit.

A BOM is a list of components that should be included with a given kit or asset type. It can be conditional on context: election type (General vs. Primary), voting-location type (Early Voting vs. Election Day), location-specific needs (ADA-required vs. standard). In practice:

- A **Polling Place Kit — Standard** might define: 2 voting machines, 1 ballot scanner, 4 privacy booths, 1 ADA booth, 1 supply box, 1 signage package.
- A **Polling Place Kit — ADA Enhanced** adds an accessible voting device or a wheelchair ramp.
- An **Early Voting Site Kit** substitutes additional laptops and ballot boxes for the early-voting volume.
- A single-asset BOM says that every deployed **Ballot Box** ships with 2 seals (one for the slot, one for the lock).
- Another says every deployed **Voting Machine** ships with 1 carrying case, 1 power cord, and 1 tablet — when it's a BMD configuration.

Once the BOMs are configured, the system uses them at two critical moments.

- **Guided preparation.** Creating a work order for a specific polling site auto-populates the work order with the items the site's BOM requires. If Precinct 12 is an ADA-designated large-precinct location, the system pre-populates the Precinct 12 kit work order with the ADA booth, the accessible voting device, and the extra booth the rule set calls for.
- **Validation.** When staff try to close a kit work order, the system checks the scanned contents against the expected BOM. *Precinct 12 kit is missing ADA booth* is surfaced as an error, not a surprise discovered on election morning.

> **In practice. Case #100 holds Voting Machine #A100, Booth #B5, and Supply Pack #S20 for Precinct 12. At 5:12 a.m. on election day, a warehouse tech scans Case #100 as it loads onto Truck 3. The system silently marks A100, B5, and S20 as on Truck 3 too. At 6:18 a.m., Truck 3 arrives at Precinct 12; the polling-place judge scans Case #100 at the door. Three items register as delivered, not just one. At close of polls, the judge scans the return version of the Precinct 12 kit — the Judge's Handoff Bag (Inbound Return) BOM expects voted ballots, two memory cards, and a results tape. The bag that returns is missing one memory card. The system flags the kit as non-compliant before the bag leaves the polling place, and the judge has a chance to find the card while there is still someone on site to help.**

Operational benefits

- **Efficient packing and handoffs.** One scan moves a group; the system handles what is inside.
- **Fewer errors.** Automated validation flags missing kit components before they become an election-day problem.
- **Flexibility.** New equipment types, pilot programs, or a change in accessibility policy are reflected by updating the rule set — next election's kits propagate automatically.
- **Traceability.** A location that reports "we were missing our ADA device" becomes a finite investigation: was it in the BOM, was it scanned during packing, was it in the case that shipped? The answer is in the system.
- **Mental-model alignment.** Warehouse staff think in "the Precinct 12 case." The system thinks the same way, without losing the individual asset view underneath.

Audit Trails and Accountability

Chain of custody, operational visibility, work orders, seals, and kit tracking all produce records. Audit trails are how those records become evidence — a permanent, attributed, tamper-evident log that an election office can show to an auditor, a court, a legislator, or the public, and defend as authentic.

Why it matters

Every previous section in this document describes a place where NxtAssets captures an event. Audit trails are where all of those events are preserved, attributed, and protected from modification. An audit trail is not a feature in its own right — it is the deliverable the rest of the platform produces.

Election records are not ordinary business records. They are retained under statute. They are subject to public inspection. They are, in an increasing number of jurisdictions, the subject of post-election challenges, risk-limiting audits, and court-ordered reviews. The system that captures them has to assume they will be scrutinized.

What gets logged

NxtAssets writes log entries for every event that touches an asset. In practice, that means:

- **Asset status changes** — *deployed, in maintenance, retired.*
- **Chain-of-custody events** — every handoff (see §1).
- **Work-order state transitions** — who marked which step complete, when (see §3).
- **Seal events** — apply, inspect, remove, replace (see §4).
- **Location updates** — every scan, every tracker ping (see §2).
- **User actions** — login, device, interface, action performed.
- **Configuration changes** — workflow edits, asset-attribute updates, role-permission changes.

Taken together, these logs form a timeline of what happened in the system and in the field — a record of activity granular enough to answer after-the-fact questions that nobody thought to ask at the time.

Why the record cannot be rewritten

Chain-of-custody events, seal events, and other critical records are stored in **write-once, append-only tables** that are cryptographically chained. Once an entry is written, it cannot be altered or deleted — not by a user, not by an administrator, not by a database administrator. A custody handoff event is chained to the ledger by a cryptographic hash; altering a timestamp or a name would break the chain, and the tampering would be evident.

The guarantee is enforced below the application layer. The database engine physically prevents the modification. The application does not offer an edit control because there is no edit path to offer.

Retention is configurable per record class and enforced the same way. Texas records retention under TEC §66.058 runs 22 months. The federal retention window under 52 USC §20701 is also 22 months. Retention can be extended through configuration; it cannot be shortened to purge records before their statutory window closes.

Accountability by name

Every user of NxtAssets has a unique login. Every action is linked to that identity. The system can answer *who did what, when.* A supervisor reviewing a late work order sees *User Jane Doe (jdoe123) marked Work Order #456 complete on Oct 30 at 3:45 p.m.* A seal-audit report notes *Technician John Smith applied Seal #789 to Scanner Unit #5 at 5:17 p.m.* Attribution is a deterrent before it is a forensic tool — staff know their actions are on the record, and behavior shifts accordingly.

> **In practice. Six weeks after the general election, a contest emerges over a close race in Precinct 12. A question is raised: was voting machine A100 opened or serviced during election day? The county attorney asks the elections office for evidence. The election director runs a single report against the immutable audit log: every seal event, every chain-of-custody event, every work-order action, every location ping for machine A100 between 5:00 a.m. and 8:00 p.m. on election day. The log shows no seal breaks, no maintenance events, no unscheduled handoffs — and it shows that the log itself has not been altered since the election, because the cryptographic chain is intact. The report goes to the county attorney with the export timestamp. The question is answered — with evidence, not with a memo.**

Audit reports and public inspection

Audit reports extract these logs in human-readable form for whatever purpose is needed: a chain-of-custody summary for a Secretary of State inquiry, a seal history for an observer request, a complete event timeline for a maintenance log sought under TEC §125.064's public-inspection window. The data is structured, so producing reports is a report run, not a sifting-through-boxes exercise.

Retention and transparency

Data retention policies are configurable per log class and enforced by the storage layer. Election records stay for at least the statutory 22 months; longer if the jurisdiction requires it. Once the window closes, retention policy governs whether records are archived or remain live. They are never purged earlier.

Transparency to oversight bodies follows from the same architecture. Election offices can share post-election custody logs with party observers, admit observers to real-time dashboards during operations, or produce read-only views for court-ordered review. Because the underlying record cannot be altered, the office is sharing evidence, not narrative.

Operational benefits

- **Forensic-quality evidence on demand.** Post-election audits, recounts, and investigations have a record to work from — not a reconstruction.
- **Faster public-records response.** Structured, attributed logs make FOIA-style requests a report run.
- **Defensible retention.** Statutory retention floors are enforced by the system; jurisdictions cannot accidentally drop records early.
- **Deterrent attribution.** Every action has a name on it. Staff know it, and conduct follows.
- **Framework alignment.** The audit architecture maps to the controls frameworks (SOC 2, NIST CSF 2.0) that administrators and auditors already speak.

Closing

Chain of custody, operational visibility, work orders and workflows, seal management, asset nesting and kits, and audit trails — these are the six concepts that shape NxtAssets in practice. Each one addresses a specific point of failure in the work of running an election: *who had this, where is it, did the steps happen, is it still sealed, did the right kit go, and can we prove it*. Taken together, they are the difference between an operation run from a spreadsheet and an operation run from a platform built for election stakes.

Every device, every box, every seal, every handoff is accounted for. Election teams operate with evidence rather than memory. Observers, auditors, and courts get answers in minutes rather than weeks.

Each concept covered here is explored in more detail in the NxtAssets User Guide and in the *NxtAssets Compliance Matrix*, which maps every statutory and standards requirement to the specific platform capability that meets it.