NxtAssets

Security Architecture

Protecting Election Data, Equipment Records, and Chain-of-Custody Integrity

Next Election Services, LLC • April 2026

Executive Summary

NxtAssets runs on Oracle Cloud Infrastructure, using Oracle's Autonomous Database and APEX application platform. This is a single-vendor, fully managed stack — the database, application server, and cloud infrastructure are all designed, maintained, and patched by Oracle. Security patches are applied automatically. There is no window where your system is waiting on someone to schedule an update.

Data Protection

All data is encrypted at rest using AES-256 encryption. This encryption is always on and cannot be turned off, even by a database administrator. Every connection to NxtAssets is encrypted in transit using TLS 1.2 or 1.3. The system will not accept an unencrypted connection. Backups are encrypted with separate keys from the live database.

Tamper-Proof Records

Chain-of-custody events, seal logs, and critical workflow records are stored in Oracle blockchain tables — a database feature that makes records physically impossible to modify or delete after they're written. Each record is cryptographically linked to the one before it, so any tampering would break the chain and be immediately detectable. Retention policies on these tables can be configured to match your statutory preservation requirements.

Access Control

NxtAssets uses role-based access control. Warehouse staff, field technicians, election site leads, administrators, and IT personnel each see only what they need and can only perform actions appropriate to their role. Every action is logged with the user's identity, a timestamp, and the device they used. The system can always answer: who did what, when, and from where.

Cloud Security Posture

Oracle Cloud Infrastructure holds SOC 1/2/3, ISO 27001, FIPS 140-2, and NIST 800-53 compliance attestations. OCI Government Cloud regions are authorized at FedRAMP High (the highest level) and DISA Impact Level 5. NxtAssets currently runs on OCI commercial regions, which carry the full certification portfolio minus FedRAMP. If your county requires FedRAMP authorization, NxtAssets can be deployed to GovCloud regions without application changes — it's a deployment configuration, not a redesign.

NES has chosen not to deploy to GovCloud by default because it carries a cost premium that most Texas counties don't need today. The option is there when a customer's security requirements or procurement rules call for it.

Regulatory Alignment

The security architecture directly supports compliance with Texas Election Code Chapter 129 (chain of custody, seal management, access control, breach recovery), EAC Chain of Custody Best Practices, and the CISA five-function cybersecurity framework. A detailed compliance crosswalk mapping specific NxtAssets capabilities to individual statutory citations is available as a companion document.

Technical Discussion

The following sections provide implementation-level detail for IT directors, security architects, and compliance officers evaluating the NxtAssets platform.

1. Platform Stack

- **Cloud Infrastructure:** Oracle Cloud Infrastructure (OCI). US-based commercial regions. OCI Government Cloud (FedRAMP High JAB P-ATO, DISA IL4/IL5) available on request.
- **Database:** Oracle Autonomous Database 23ai. Fully managed, self-patching, self-securing. Automated security patch application eliminates manual patching windows.
- **Application:** Oracle APEX 24.2. Runs entirely within the Oracle Database — no separate application server. Stateless HTTP with server-side session management.
- **IoT / Tracking:** Oracle OCI Cloud IoT Service for GPS and Bluetooth tracking device management, hosted on OCI.
- **Uptime SLA:** OCI compute and database: 99.995%.

2. Encryption

2.1 At Rest

- **Mechanism:** Transparent Data Encryption (TDE) with AES-256 tablespace encryption.
- **Enforcement:** TDE is enabled by default on Oracle Autonomous Database and cannot be disabled. This is not a configuration option — it is a platform invariant.
- **Key Management:** Each database instance has a unique master encryption key. Backups use separate encryption keys. Keys stored in PKCS#12 keystore on the database host.
- **Key Rotation:** Supported and configurable to meet organizational rotation policies.

2.2 In Transit

- **Protocol:** TLS 1.2 and TLS 1.3. TLS 1.3 is the default on Oracle Database 23ai.
- **TCPS Connections:** Certificate-based mutual authentication via connection wallet. Wallet distribution is controlled — only authorized clients receive credentials.
- **TCP Connections:** Oracle Native Network Encryption with mandatory AES-256/192/128 negotiation.
- **Enforcement:** Unencrypted connections are rejected at the server level. This server-side configuration cannot be changed by administrators or users.

3. Immutable and Blockchain Tables

NxtAssets uses Oracle 23ai blockchain tables for chain-of-custody events, seal logs, and other critical audit records. These are insert-only tables with cryptographic integrity guarantees.

- **Insert-Only:** DELETE, UPDATE, and TRUNCATE operations are rejected by the database engine with ORA-05715. This is enforced at the kernel level, not the application level.
- **Cryptographic Chaining:** Each row stores a SHA2-512 hash of its data plus the hash of the previous row, forming a verifiable chain. Tampering with any row breaks the chain and is detectable via DBMS_BLOCKCHAIN_TABLE.VERIFY_ROWS.
- **User Signatures:** Optional user-level digital signatures can be stored per row for additional non-repudiation.
- **Retention Policies:** Configurable via NO DROP UNTIL n DAYS IDLE and NO DELETE UNTIL n DAYS AFTER INSERT clauses. Can be set to match statutory retention periods (e.g., 22 months per TEC §129.024(b), §66.058).
- **Immutable Tables:** Used where insert-only protection is needed without the overhead of cryptographic chaining (e.g., non-critical operational logs). Same insert-only, no-delete semantics without hash columns.

3.1 Unified Auditing

Oracle Unified Auditing is always-on in Database 23ai. Traditional auditing is no longer supported.

- **Audit Trail:** Stored in the AUDSYS schema in the AUD$UNIFIED table. This table allows only INSERT — any attempt to truncate, delete, or update fails and itself generates an audit record.
- **Protection:** Audit tablespace can be encrypted with TDE. Audit table can be protected with Oracle Database Vault realm. UNIFIED_AUDIT_SYSTEMLOG parameter writes key audit fields to syslog in parallel.

- **Scope:** Captures unified audit policies, fine-grained audit records (DBMS_FGA), Real Application Security records, and APEX session-level activity.
- **Predefined Policies:** Oracle Autonomous Database enables multiple audit policies by default, including ORA_SECURECONFIG and ORA_LOGON_FAILURES. Additional policies configurable per county requirements.

4. Access Control and Identity

4.1 Infrastructure Level (OCI IAM)

- **Identity Federation:** OCI IAM supports federation with external identity providers (SAML 2.0, OIDC). MFA available.
- **Compartments:** OCI resources are isolated in compartments with policy-based access. NxtAssets infrastructure is segregated from other OCI tenancy resources.
- **API Audit:** All OCI control plane operations (create, modify, delete resources) are logged by the OCI Audit service regardless of interface (Console, CLI, SDK, REST API).

4.2 Application Level (Oracle APEX)

- **Authentication:** Configurable schemes: database accounts, LDAP, Oracle SSO, social sign-in, custom PL/SQL. NxtAssets uses database authentication with county-specific configuration.
- **Authorization:** Granular control at application, page, region, button, and item level. Dynamic authorization via PL/SQL conditions. Row-level security supported for multi-tenant or role-restricted data access.
- **Session Management:** Server-side sessions stored in database tables (not client-side). Configurable session timeout and idle limits. Session state protection via cryptographic checksums prevents URL parameter manipulation.
- **CSRF Protection:** Built-in token-based protection against cross-site request forgery.

4.3 NxtAssets Role Model

NxtAssets defines application roles with least-privilege access: System Administrator, Warehouse Operations, Field Technician, Election Site Lead, IT/Reporting, Auditor (read-only), Service Desk. Roles are configured per implementation and can be extended with attribute-based constraints (e.g., location, election, time period).

5. Application Security

- **XSS Prevention:** APEX escapes all output by default. The APEX Advisor tool scans applications for settings that could reduce security.
- **SQL Injection Prevention:** APEX uses bind variables by design. Oracle 23ai SQL Firewall provides additional runtime protection: inspects all incoming SQL (including PL/SQL, local, network, encrypted, cleartext) and allows only explicitly authorized statements.
- **URL Integrity:** Session State Protection enforces cryptographic checksums on URL parameters. Bookmarked or manipulated URLs without valid checksums are rejected.
- **Sensitive Data in Session:** Session state values for sensitive items can be stored encrypted in APEX session management tables. Restricted items cannot be set from browser-side parameters.
- **Auto-Patching:** Oracle Autonomous Database applies Critical Patch Updates automatically. No county IT action required for infrastructure and database security updates. APEX is patched as part of the managed database service.

6. OCI Security Services

- **Cloud Guard:** Automated threat detection and response. Monitors for misconfigured resources, insecure activity, and malicious threats across the OCI tenancy. Detector recipes identify problems; responder recipes can auto-remediate.
- **OCI Vault:** FIPS 140-2 Level 3 validated HSMs for customer-managed key storage. Available if county policy requires keys to be managed outside the database host.
- **VCN Security:** Virtual Cloud Networks with security lists and Network Security Groups. VCN Flow Logs provide traffic monitoring (source, destination, quantity, permit/deny) for compliance and forensic analysis.
- **Data Safe:** Integrated database security assessment, activity auditing, data discovery, and data masking. Included with Autonomous Database subscription.
- **Bastion Service:** Provides time-limited, audited SSH access for administrative sessions without exposing hosts to the public internet.

7. Compliance Attestations

OCI commercial regions carry the following independent third-party attestations:

- SOC 1 Type II, SOC 2 Type II, SOC 3
- ISO 27001:2013, ISO 27017 (Cloud Security), ISO 27018 (Cloud Privacy)
- FIPS 140-2 validated cryptographic modules
- NIST 800-53 high-impact baseline (assessed as part of FedRAMP)
- PCI DSS, HIPAA, GDPR, C5, IRAP, MTCS

OCI Government Cloud regions add:

- FedRAMP High JAB P-ATO (93+ authorized services)
- DISA Impact Level 4 and Impact Level 5 (IL5 PATO)

NxtAssets currently deploys to OCI commercial regions.

GovCloud deployment w/ FedRAMP and TxRAMP compliance available at extra cost.

8. Regulatory Mapping

The NxtAssets Compliance Crosswalk (available separately) provides a mapping of specific regulatory citations to NxtAssets capabilities. Coverage includes:

- **Texas Election Code:** §§129.051–.053 (pre-election security, transport, access control), §129.024 (seal/test material security), §§125.002–.006 (equipment prep through closeout), §§127.061–.069 and .123/.154–.155 (sealed ballot boxes, tabulation equipment IDs), §§66.021/.058/.062 (precinct records and retention).
- **EAC:** Chain of Custody Best Practices (2021), Best Practices for Election Technology (Physical Security), Equipment Disposal Guidance.
- **CISA:** Chain of Custody and Critical Infrastructure Systems (2021), Physical Security Checklist, NIST CSF alignment across all five functions (Identify, Protect, Detect, Respond, Recover).
- **TX SOS:** Advisory 2019-23 and Advisory 2012-03 (Electronic Voting System Procedures).

For a security briefing or technical deep-dive with your IT team:

Next Election Services, LLC | (855) 728-6398 | info@nxtelection.com | nxtelection.com