SECURITY WHITE-PAPER -- VERSION 2026.3

Security & Data Trust Architecture Whitepaper

Technical, administrative, and physical safeguards engineered to secure your property archives and ensure complete data sovereignty.

OVERVIEW

Executive Summary

Cadastre Home provides a forensic, permanent digital record of residential and commercial property assets to secure insurance claim readiness before disasters occur. Because our platform houses complete interior spatial layouts, asset values, serial numbers, and 360-degree media, we treat data security not as an operational feature, but as our foundational platform dependency. This document details the technical, administrative, and physical safeguards engineered into Cadastre Home to ensure complete user sovereignty and data confidentiality.

TIER 1 SAFEGUARDS

1. Data Encryption Architecture

Cadastre Home isolates data at every point in the collection, transit, and storage life cycle.

- Data in Transit: All communications between user client devices running our native mobile application, external capture hardware, and our infrastructure are encrypted using Transport Layer Security (TLS 1.3) protocols.
- Data at Rest: All property inventories, values, metadata, and core application tables are stored within isolated cloud database clusters utilizing Advanced Encryption Standard with a 256-bit key length (AES-256).
- Media Security: Raw property imagery, 360-degree virtual tours, and document uploads are stored within private, access-controlled AWS Simple Storage Service (S3) buckets. Media assets are completely unindexed publicly and cannot be fetched via standard URLs.

> Secure Media Access Rule: Media can only be accessed via cryptographically signed, time-limited URLs generated programmatically for an active, authenticated user session, or user-generated, tamper-verified public share tokens (revocable instantly via the dashboard).

ACCESS CONTROLS

2. Multi-Tenant Isolation & Access Control

We eliminate the risk of cross-account data leaks through rigorous database engineering.

- Row-Level Security (RLS): Our database architecture relies on strict Postgres Row-Level Security via Supabase. Every query executed against the database is programmatically bound to the user's cryptographically verified authentication token (auth.uid()). One user account cannot query, see, or accidentally receive structural tables or records belonging to another account.
- Administrative Access Isolation: Cadastre Home personnel do not have blanket access to read vault contents. System administrators can only view account infrastructure metrics and metadata. Access to raw property vaults for technical troubleshooting requires explicit, time-locked authorization logging.

DEVICE PROTECTIONS

3. Application-Enforced Hardware Protections

Whether utilizing our professional Concierge capture services or documenting a property as a DIY subscriber, specialized hardware data controls are programmatically enforced by our mobile app:

- Zero Native Device Retention: The Cadastre Home mobile capture application completely bypasses the device’s public media library. Images captured via onboard device lenses are isolated entirely within the application's private, secure storage sandbox and are completely flushed immediately following server upload verification.
- SDK-Driven Camera Sanitization: For users and partners connecting standalone 360-degree hardware (such as Insta360 arrays), our app interfaces directly with the hardware logic board via official mobile SDKs. The raw data stream is extracted securely through the app sandbox and sent straight to our cloud vault. The moment the server confirms safe ingestion, the app transmits an immediate command back to the camera to wipe the file from the hardware storage card.
- Background and Vetting Standards: Every Certified Capture Partner entering a property is fully vetted, background-checked, and bound by comprehensive non-disclosure and strict automated data non-retention agreements.

RESILIENCE

4. Infrastructure Resilience and Continuity

Our infrastructure is built to survive regional disaster events without compromising client records.

- Data Redundancy: Databases are continuously backed up using multi-region point-in-time recovery mechanisms. Backups are completely encrypted at rest and retained for 30 days to ensure resilience against localized natural disasters affecting data centers.
- Hosting Standards: All platform infrastructure is hosted within SOC 2 Type II, ISO 27001, and PCI-DSS compliant datacenters operated by Amazon Web Services and Supabase in secure domestic United States regions.

> *Disclaimer: This whitepaper details security controls implemented across the Cadastre Home SaaS platform. Security standards and system configurations are subject to scheduled audits and updates. Contact security@cadastrehome.com for detailed compliance requests.*