

Security Overview

Effective Date: June 2026 · Version 1.0

VouchVid is designed with security as a foundational principle. This document summarises the administrative, technical, and organisational controls in place to protect dealership and customer data.

1. Infrastructure & Hosting

- **Cloud hosting:** All application infrastructure runs on Google Cloud Platform (GCP), a SOC 2 Type II and ISO 27001 certified provider.
- **Database:** Customer and video metadata is stored in Google Cloud Firestore with server-side encryption at rest.
- **Video storage:** Video files are stored on Cloudinary, which provides encrypted delivery via HTTPS/TLS 1.2+ on all media assets.
- **Geographic redundancy:** Data is replicated across multiple availability zones to ensure uptime and resilience.

2. Data Encryption

Layer	Standard
Data in transit	TLS 1.2 / TLS 1.3 (all endpoints)
Data at rest	AES-256 (Firestore & Cloudinary)
Video delivery	HTTPS-only signed URLs
Authentication tokens	Firebase Auth / short-lived JWTs

3. Access Control

- Role-based access control (RBAC): admin, member, and group-owner roles with separate permissions
- Authentication via Firebase Auth — no shared credentials
- Admin PIN required to access kiosk management interface on-device
- All Firestore security rules restrict read/write to authenticated users scoped to their account
- Group portal access is isolated per dealer group — cross-group data access is architecturally prevented

4. Application Security

- Input validation on all form fields and API endpoints
- No third-party advertising SDKs or tracking pixels in the kiosk application
- Content Security Policy (CSP) headers on all web-facing pages
- Dependency audits performed prior to major releases
- Cloudinary upload presets enforce file-type restrictions (video only on kiosk endpoints)

5. Incident Response

In the event of a confirmed data security incident, VouchVid will notify affected dealership account administrators within 72 hours of discovery. Notification will include the nature of the incident, data categories affected, and remediation steps taken.

6. Vendor Security

All third-party sub-processors are evaluated for security posture prior to integration. VouchVid maintains a current Sub-Processor Register listing all vendors with access to customer data and their applicable certifications.

7. Contact

To report a security concern or request documentation: privacy@vouchvid.com · vouchvid.com