# SimpleSafe™

## Security & Data Protection Overview

*How SimpleSafe safeguards your organization's data and incident documentation across the platform.*

SimpleSafe is built on enterprise-grade cloud infrastructure with a security-first architecture: customer data is isolated by organization, access is denied by default, and every automated process authenticates with short-lived credentials rather than stored secrets. The summary below reflects the controls in place across the SimpleSafe™ platform.

---

HOSTING & ENCRYPTION

### Google Cloud foundation

The platform runs on Google Cloud (Firebase). All data is encrypted in transit (TLS) and at rest by default using Google-managed encryption, inheriting Google Cloud's physical, network, and infrastructure security.

ACCESS CONTROL

### Deny-by-default isolation

Each organization's data is logically isolated from every other tenant. Database rules are deny-by-default — no record is reachable unless access is explicitly authorized for that specific account.

AUTHENTICATION

### Short-lived tokens, no stored secrets

Backend automations authenticate using short-lived service-account tokens (roughly 30-minute lifespan), not static passwords or shared keys. No long-lived downloaded credential files exist anywhere in the environment.

CREDENTIAL HYGIENE

### Least privilege by design

A single, least-privileged service identity handles backend operations, scoped only to what it needs. Keys are rotated on a defined cadence, and unused accounts and credentials are retired.

THE SIMPLESAFE DIFFERENTIATOR

### Legal-grade chain of custody for incident records

Incident documentation captured through SimpleSafe is transmitted in real time to an independent Dallas-based premises-liability law firm that acts as legal custodian, returning a timestamped acknowledgment of receipt. This establishes a verifiable record outside your organization's own systems from the moment an incident is logged.

PAYMENT SECURITY

### Card data never touches SimpleSafe

- Payments processed by Stripe (PCI-DSS Level 1 certified)
- Cardholder data flows directly to Stripe — SimpleSafe neither stores nor handles it
- No payment card information resides in SimpleSafe systems

DATA WE HANDLE

### A deliberately small footprint

- Incident reports and staff activity records
- Manager Portal account and usage data
- No medical records or consumer financial data stored

---

### Working with your security & procurement team

SimpleSafe is glad to complete vendor security questionnaires (SIG, CAIQ, or your own format) and provide additional documentation on request. If your organization requires specific assessments or evidence as part of onboarding, we'll work with your team to provide what you need.