



Security & Data Protection Overview

How PGI safeguards course data, staff certification records, and incident documentation across its platform.

PGI is built on enterprise-grade cloud infrastructure with a security-first architecture: customer data is isolated by course, 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 SimplePace, SimpleSafe, and certification systems.

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 course'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. Isolation is enforced at the data layer and verified.

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, authentication is monitored, and unused accounts and credentials are retired.

THE PGI DIFFERENTIATOR

Legal-grade chain of custody for incident records

Incident documentation captured through PGI 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 the course's own systems from the moment an incident is logged — supporting insurance and legal defensibility in a way standard documentation tools do not.

PAYMENT SECURITY

Card data never touches PGI

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

DATA WE HANDLE

A deliberately small footprint

- › Operational data: pace-of-play and staff-interaction records
- › Staff certification and training records
- › Course-submitted incident reports
- › No medical records or consumer financial data stored

Working with your security & procurement team

PGI 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.