Security Overview

For brokerages, MGAs and carriers reviewing PolicyStream. PolicyStream collects life insurance applications, including health history and banking details, so we treat every field as sensitive.

HOSTING AND DATA RESIDENCY

- Amazon Web Services, Canada (Central) region (ca-central-1). The database, uploaded files, backups, sign-in accounts (Amazon Cognito) and transactional email (Amazon SES) are all in Canada.
- Production runs in its own dedicated AWS account, separate from testing.
- Exceptions: requests pass through Amazon CloudFront edge locations (encrypted, not stored). Firewall logs of blocked or flagged requests are kept 30 days in AWS US East, the only region where AWS offers that firewall for CloudFront.

ENCRYPTION

- In transit: TLS 1.2 or newer on every public endpoint, and HTTP is redirected to HTTPS. Database connections require TLS.
- At rest: the database, file storage and backups are encrypted with AWS KMS keys. Application secrets live in AWS Secrets Manager, never in source code.

IDENTITY AND ACCESS

- Passwords are at least 12 characters long and mix upper case, lower case and numbers.
- Two-step sign-in uses an authenticator app (TOTP). There's no SMS fallback.
- Two-step sign-in is mandatory for owners and admins of any workspace with 2+ people.
- Roles: owner, admin, advisor and assistant. Advisors and assistants see only the clients assigned to them.
- The app signs users out after 30 minutes idle, and sessions end after 12 hours. Trusted devices expire after 30 days.
- Changing a password or email requires signing in again.
- No "view as advisor" or staff back-door screen exists in the product.
- Tenant isolation is enforced by row-level security in the database, with cross-tenant tests in CI.

CLIENT LINKS AND DOCUMENTS

- Client links use random 192-bit tokens that are stored only as hashes and expire after 30 days. The first device is bound with a server-issued random device ID in an HttpOnly, Secure, SameSite=Strict cookie (only its hash is stored). On any other device, the client confirms their identity with an emailed one-time code (10-minute life, rate-limited). After 5 wrong codes, new-device verification locks until the advisor reissues the link; the trusted device keeps working.
- Clients are emailed when an application is first started and after any new device is verified (device type and time), so unexpected access is visible to them. These emails never contain answers.

- Submitted answers are locked and versioned. Compliance documents are frozen at send time and fingerprinted with SHA-256.
- Signature evidence records the typed name, timestamp, IP and browser, in an append-only trail.

MONITORING, LOGGING AND RESILIENCE

- A web application firewall (AWS WAF) runs AWS managed rules plus rate limits. CloudWatch alarms cover error rates, latency, failed sign-in surges, database health and email bounces.
- An organization-wide AWS CloudTrail logs every administrative action across all accounts, in all regions, with log-file integrity validation. The logs are kept for a year, locked against changes, in a separate AWS account that our application and deploy tools can't reach.
- Administrator sign-in to our AWS accounts uses single sign-on with 2-step verification and one-hour sessions. Root logins have 2-step verification and are kept for emergencies only.
- AWS Security Hub checks our configuration daily against the AWS Foundational Security Best Practices standard, and AWS GuardDuty watches for threats.
- The production database is Multi-AZ PostgreSQL. It keeps 30 days of automated, point-in-time backups and has deletion protection on. Every night, AWS Backup also copies the database and file storage into a locked vault in a separate AWS account (Canada Central), so backup copies can't be deleted early.
- Restore drills run quarterly on production. The first one, on 2026-09-28, passed: the restore took 10.6 minutes and lost 2.6 minutes of data at most.

SOFTWARE DEVELOPMENT

- Every change goes through a reviewed pull request, with automated tests (including cross-tenant isolation tests), dependency auditing (npm audit, Dependabot) and secret scanning (gitleaks).
- Deployments use GitHub OIDC with no stored cloud keys. Production deploys are manual and approved.
- Security testing: in October 2026 we ran two rounds of authorized, hands-on testing against our staging environment, covering workspace isolation, sign-in and sessions, client links, uploads, integrations and embedding. Confirmed issues (a session that kept working after sign-out, and a missing warning on unverified connected apps) were fixed and verified in a retest. Remaining items are low-risk hardening on our roadmap.

PAYMENTS

- Advisors' subscription cards are entered in Helcim's hosted payment form (HelcimPay.js). PolicyStream never receives or stores card numbers or CVV. Banking details that clients enter in applications are encrypted with the rest of the application and passed to the carrier the advisor chooses.

PRIVACY

- Designed around PIPEDA and the Alberta and BC privacy acts. The advisor/brokerage controls client data; PolicyStream acts as their service provider.
- No sale of data, no advertising use, no analytics on client data.
- Data can be exported at any time. After a workspace closes, there's a 30-day export window, then data is permanently deleted, including every stored file version.

- Breaches are recorded for 24 months. Affected brokerages are notified without delay, and we support them in notifying clients and the Privacy Commissioner.

SERVICE PROVIDERS

PROVIDER	PURPOSE	LOCATION
Amazon Web Services	Hosting, database, files, backups, sign-in, email	Canada (Central)
Cloudflare	DNS, marketing site, routing for advisors' own quote domains (pass-through)	Global network
Helcim	Subscription billing (advisor cards)	Canadian processor
Google Workspace	PolicyStream's own support email	Google data centres

COMPLIANCE STATUS

ITEM	STATUS
PIPEDA / Alberta PIPA / BC PIPA programme	**In place**
Canadian data residency	**In place**
Quarterly backup restore drills	**In place**
PCI DSS scope minimised (hosted payment form)	**In place**
Active security testing (two rounds, October 2026; all confirmed findings fixed and retested)	**Completed**
Technology E&O (professional liability) and cyber liability insurance	**In place**
SOC 2 Type I	**Planned**

> **Shared responsibility.** PolicyStream secures the platform. The advisor/brokerage is responsible for client consent and their privacy notice, for reviewing answers before submission, for suitability and disclosure, for their licensing obligations, and for keeping logins and devices secure.

Questions, questionnaires or document requests: philip@policystream.ca · Security issues: support@policystream.ca · Privacy Officer: Philip Setter · www.policystream.ca/security/
This overview describes controls in place as of the version date and is provided for information. It doesn't amend the PolicyStream Terms of Service.