SECURITY & TRUST

Security & Trust Overview

SOC 2 readiness & controls summary for PortLens

PortLens (sole trader) · ABN 59 498 934 467 · Australia | Prepared by PortLens | Last updated 16 August 2026 | v1.0

Important — please read

This Security & Trust Overview is a **self-assessment prepared by PortLens**. It describes our current security controls presented against the AICPA SOC 2 Trust Services Criteria. **It is not an independent SOC 2 examination and contains no auditor's opinion.** PortLens has not yet completed a SOC 2 Type I or Type II audit by a licensed CPA firm. A formal, independent SOC 2 Type II examination is on our roadmap as the business scales (see Section 8). Until then, this document is intended to give customers and partners an honest, transparent view of how we protect data today.

1. About PortLens & this document

PortLens is a portfolio-risk copilot for investors in Australian Securities Exchange (ASX) listed companies, with on-demand support for global securities. It helps investors understand the risk exposures in a portfolio they enter — it does not execute trades, hold client money, or access brokerage accounts. This document describes the technical and organisational controls PortLens uses to protect customer information, organised against the SOC 2 Trust Services Criteria (TSC).

2. Scope & Trust Services Criteria

This overview covers the PortLens web application, its API and supporting cloud infrastructure. It is presented against three Trust Services Criteria commonly requested of fintech vendors:

- **Security** — systems are protected against unauthorised access.
- **Availability** — the service is reliable and available as intended.
- **Confidentiality** — customer information is protected and access-restricted.

Processing Integrity and Privacy are not formally in scope for this readiness overview, though PortLens's privacy practices are summarised in Section 6 and in our published Privacy Policy.

3. Security controls

Control	How PortLens addresses it	Criteria
Authentication	Accounts are protected with token-based authentication (signed JWTs, HS256). Sessions expire automatically and require re-authentication.	Security
Password storage	Passwords are hashed with bcrypt using a unique per-password salt. Plaintext passwords are never stored or logged.	Security
Encryption in transit	All traffic is served exclusively over HTTPS/TLS, terminated at a hardened edge (Cloudflare) in front of the application.	Security · Conf.
Secrets management	API keys, database credentials and signing secrets are held only in server-side environment configuration — never hardcoded in source or exposed to the browser.	Security

Control	How PortLens addresses it	Criteria
Input validation	Every API request is validated and type-constrained (Pydantic schemas) before processing, reducing injection and malformed-input risk.	Security
Access control	Feature and administrative access is enforced by an entitlement layer (least-privilege); owner/administrative functions are segregated from standard user access.	Security · Conf.
Payment data	Card payments are handled entirely by Stripe (PCI-DSS Level 1). PortLens never receives, processes or stores card numbers; Stripe webhooks are signature-verified.	Security · Conf.
Cross-origin policy	Browser access is restricted by a configurable CORS allowlist scoped to the PortLens domain in production.	Security

4. Availability controls

Control	How PortLens addresses it	Criteria
Managed infrastructure	The application runs on managed, containerised cloud infrastructure with a content-delivery/edge network (Cloudflare) providing DDoS protection and caching.	Availability
Managed database	Customer data is stored in a managed MongoDB service with provider-level redundancy and durability.	Availability
Logging & monitoring	Application events are logged; operational metrics and error signals are surfaced on an internal monitoring dashboard for the operator.	Availability
Graceful degradation	External data providers (market data, FX, email, AI) are wrapped with timeouts and fallbacks so a single dependency failure does not take down the service.	Availability

5. Confidentiality controls

Control	How PortLens addresses it	Criteria
Data minimisation	PortLens collects only what it needs to operate: account email & name, a hashed password, and the portfolio holdings a user chooses to enter. It does not collect bank logins, card numbers, or government identifiers.	Confidentiality
Segregation of data	Each user's portfolio and options data is scoped to their account and is not shared with other users.	Confidentiality
No sale of data	PortLens does not sell customer data. Analytics are consent-gated and aggregated.	Confidentiality · Privacy
Restricted access	Access to production data is limited to the operator on a need-to-know basis.	Confidentiality

6. Data we process & privacy

PortLens processes: (a) **account data** — email address, display name and a bcrypt-hashed password; (b) **portfolio data** — the tickers, quantities, cost bases and option positions a user enters; and (c) **usage data** — consent-gated, aggregated analytics. Payment/billing identifiers are held by Stripe. Users may request access to, correction of, or deletion of their personal information by contacting us. Full detail is in the PortLens Privacy Policy and Cookie Policy.

7. Sub-processors

PortLens relies on the following reputable providers to deliver the service. Each is bound by its own security and data-protection commitments.

Sub-processor	Purpose	Data & safeguard
Cloudflare	Edge network, TLS, DDoS protection	Encrypted traffic; no persistent customer records.
MongoDB (managed)	Primary application database	Account & portfolio data; provider redundancy/backups.
Stripe	Payments & subscription billing	Card data & billing (PCI-DSS L1); PortLens stores no card numbers.
Resend	Transactional & nurture email	Recipient email address & message content.
Emergent	Application hosting & managed AI gateway	Runs the app; brokers AI requests to model providers.
Anthropic / OpenAI	AI text generation (via Emergent)	Prompt context for briefs/research; no credentials sent.
ElevenLabs / OpenAI	Text-to-speech (audio briefs)	Brief text converted to audio on request.
Yahoo Finance	Market prices & FX rates	Public market data only; no customer data sent.
Microsoft Clarity	Product analytics (consent-gated)	Aggregated behavioural metrics; loads only after consent.

8. Roadmap to a formal SOC 2 Type II

PortLens is committed to maturing its security programme. Planned enhancements — not yet in place — include:

• Multi-factor authentication (MFA) for user and administrative access.
• Rate limiting and automated brute-force / anomaly protection on authentication endpoints.
• A documented policy suite (information security, access control, incident response, business continuity and vendor-risk policies).
• Independent penetration testing and a recurring vulnerability-scanning cadence.
• Formal backup-restoration and disaster-recovery testing with documented evidence.
• Engagement of a licensed CPA firm for an independent **SOC 2 Type II examination**, at which point this self-assessment will be superseded by the auditor's report.

9. Requesting more information

We're happy to answer security questionnaires and share further detail under a mutual NDA. For security matters, disclosures or vendor due-diligence, contact **security@portlens.com.au**. To report a suspected vulnerability, please email the same address with the details and steps to reproduce.