INFORMATION SECURITY

ISO/IEC 27001 Alignment

How PortLens aligns to ISO/IEC 27001:2022 — an ISMS readiness overview

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

Important — please read

This ISO/IEC 27001 Alignment Overview is a **self-assessment prepared by PortLens**. It describes how our information-security practices align to the ISO/IEC 27001:2022 standard and its Annex A controls. **PortLens is not ISO/IEC 27001 certified.** An ISO 27001 certificate can only be issued by an accredited certification body following a formal audit of an Information Security Management System (ISMS); no such certificate has been issued to PortLens. Certification is on our roadmap (see Section 8). This document is intended to give an honest, transparent view of our current security management practices, with each Annex A theme marked **In place**, **Partial** or **Planned**.

1. About PortLens & this document

PortLens is a portfolio-risk copilot for ASX-listed and global securities. It helps investors understand the risk exposures in a portfolio they enter; it does not execute trades or hold client money. This document maps our information-security practices to ISO/IEC 27001:2022 — the international standard for an Information Security Management System (ISMS) — so customers and partners can gauge our maturity and direction.

2. Our information-security approach (ISMS)

ISO 27001 is built around a management system rather than a fixed list of features. PortLens operates a lightweight ISMS appropriate to a sole-trader business, following the Plan-Do-Check-Act cycle: we identify the information assets we hold, assess the risks to them, apply proportionate controls (Section 6), and review and improve those controls as the product and threat landscape evolve. Formal, fully-documented ISMS artefacts (policy suite, risk register, Statement of Applicability, internal-audit and management-review records) are in development ahead of a future certification audit.

3. Scope of the ISMS

The intended scope is the development and operation of the PortLens cloud-based web application, its API and supporting cloud infrastructure, operated by a single owner-operator in Australia. Physical data-centre security is inherited from our cloud sub-processors (Section 7). This scope is what a future certificate would be expected to cover.

4. Risk management

We identify the principal information assets — customer account data, user-entered portfolio data, authentication secrets and application source code — and the threats to them, including data breach, credential theft, third-party/cloud outage, ransomware, and loss or compromise of an operator device. Each threat is treated by proportionate technical and organisational controls (encryption in transit, hashed credentials, environment-isolated secrets, managed/redundant infrastructure, least-privilege access and consent-gated analytics). A formally documented, version-controlled risk register is being established as part of ISMS formalisation.

5. Continual improvement

Security is reviewed as part of our development lifecycle: changes are validated before release, dependencies and external providers are monitored, and controls are revisited as new features (for example options analytics and global-securities support) are added. Planned enhancements are listed in Section 8.

6. Annex A controls — organizational

Control theme	How PortLens addresses it	Status
Policies for information security	Core security practices are defined and applied; a formally documented, signed policy suite is being written.	**Partial**
Roles & responsibilities	Security ownership rests clearly with the owner-operator.	**In place**
Supplier / sub-processor management	Reputable providers with their own security commitments are used and listed publicly (Section 7); a formal vendor-risk process is being documented.	**Partial**
Asset management	Key information assets are identified; a formal, maintained asset register is planned.	**Partial**
Access control policy	Least-privilege access is enforced technically via an entitlement layer; a written access-control policy with periodic reviews is planned.	**Partial**
Incident management	Issues are triaged and remediated by the operator; a documented incident-response plan with defined severities and timelines is planned.	**Planned**

7. Annex A controls — people

Control theme	How PortLens addresses it	Status
Security awareness	The single owner-operator maintains current security knowledge; a formal training programme applies if the business hires.	**In place**
Screening / onboarding / termination	Not applicable to a single operator today; background checks and joiner/leaver access procedures will be formalised upon hiring.	**N/A**
Confidentiality / acceptable use	Confidentiality obligations are honoured; written agreements will be introduced with any contractor or employee.	**Partial**

8-continued below

Annex A controls — physical

Control theme	How PortLens addresses it	Status
Data-centre / server physical security	Inherited from cloud sub-processors, which operate certified, access-controlled data centres.	**In place**
Endpoint / office security	No corporate office; the operator device is kept patched and access-protected. Formal device-management policy is planned.	**Partial**

Annex A controls — technological

Control theme	How PortLens addresses it	Status
Encryption in transit	All traffic served over HTTPS/TLS, terminated at a hardened edge (Cloudflare).	**In place**
Authentication	Token-based auth (signed JWTs) with automatic session expiry.	**In place**
Credential protection	Passwords hashed with bcrypt and unique salts; never stored in plaintext.	**In place**
Secrets management	Keys and credentials held only in server-side environment configuration.	**In place**
Secure development	Input validated/type-constrained on every request; changes reviewed before release.	**In place**
Logging & monitoring	Application events logged; operational metrics surfaced on an internal dashboard.	**Partial**
Backup	Managed database provider redundancy/backups; documented restoration testing is planned.	**Partial**
Multi-factor authentication	Not yet available for user/admin accounts; planned.	**Planned**
Vulnerability management	Dependencies monitored; independent penetration testing & scheduled scanning planned.	**Planned**
Payment data isolation	Card data handled entirely by Stripe (PCI-DSS L1); PortLens stores no card numbers.	**In place**

7. Sub-processors

PortLens relies on the following providers, each bound by its own security and data-protection commitments (see the SOC 2 / Security overview for full detail): Cloudflare (edge/TLS), MongoDB (managed database), Stripe (payments, PCI-DSS L1), Resend (email), Emergent (hosting & AI gateway), Anthropic/OpenAI (AI text), ElevenLabs/OpenAI (text-to-speech), Yahoo Finance (market data) and Microsoft Clarity (consent-gated analytics).

8. Roadmap to ISO/IEC 27001 certification

• Complete the documented ISMS: information-security policy suite, risk register, asset register and Statement of Applicability.
• Introduce MFA, rate limiting and formal access reviews.
• Establish incident-response, business-continuity and disaster-recovery plans with tested evidence.
• Commission independent penetration testing and continuous vulnerability scanning.
• Run an internal audit and management review, then engage an accredited certification body for a Stage 1 / Stage 2 **ISO/IEC 27001:2022 certification audit**. Upon certification this overview will be superseded by the issued certificate and Statement of Applicability.

9. Requesting more information

We're happy to complete security questionnaires and share further detail under a mutual NDA. For security, disclosures or due-diligence, contact **security@portlens.com.au**.