ISO and Australian Standards

How Senua AI's software and the way we build it map to ISO/IEC 27001:2022, adopted in Australia as AS/NZS ISO/IEC 27001:2023, and to the other cyber security standards Standards Australia names in its position paper "Cyber Security Standards" (January 2025). This is our own mapping; Senua AI's information security management system is being prepared for certification, dated on the assurance roadmap.

ISO/IEC 27001 Annex A: technological controls

Control	How we meet it	Status
8.2 Privileged access rights	Capabilities enforced by the engine; multi-factor sign-in required for every privileged account	Met
8.3 Information access restriction	Access by capability; your data never leaves your install	Met
8.4 Access to source code	Private repositories; every change reviewed and recorded	Met
8.5 Secure authentication	PBKDF2-HMAC-SHA-256 at 600,000 iterations with a per-user salt; lockout at five failures; one-time codes; passkeys planned	Met
8.7 Protection against malware	Signed, verified and encrypted releases; no third-party code imported	Met
8.8 Management of technical vulnerabilities	Fixes as signed releases at no charge, to the root cause; disclosure policy and independent testing planned	Partly met
8.9 Configuration management	Declared, sealed settings, each change audited; hardening guide planned	Partly met
8.10 Information deletion	All data is in your environment; uninstall tested with every release	Your environment
8.12 Data leakage prevention	Nothing leaves your install; optional check-in is off by default	Met
8.15 Logging	A tamper-evident audit log of every administrative action	Met
8.16 Monitoring activities	The software watches Senua AI's own sites, in report-only mode	Met
8.19 Installation of software	One-command installer; each bundle verified before unpacking	Met
8.20 to 8.22 Network security and segregation	One network listener; the engine on the local host; our hosted sites behind CloudFront, a load balancer and a web application firewall	Met
8.24 Use of cryptography	Every algorithm public in the cryptographic register, with a dated quantum-safe plan	Met
8.25 Secure development life cycle	A written development process: requirements, design, checks registered before code, review of every change	Met
8.26 Application security requirements	Each requirement written with its acceptance test	Met
8.27 Secure architecture and engineering	Design notes before code	Met
8.28 Secure coding	Our own language, with written rules and lint gates	Met
8.29 Security testing	Test suites, published test vectors, test installs on fresh hosts; independent penetration testing planned	Partly met
8.30 Outsourced development	None: all development is in-house, in Australia	Not applicable

Control	How we meet it	Status
8.31 Separation of environments	Build, test and production hosts kept apart; releases promoted byte for byte	Met
8.32 Change management	Each change registered with its checks before the code, recorded when it lands	Met
8.33 Test information	Public datasets and synthetic data; no customer data in testing	Met

ISO/IEC 27001 Annex A: organisational controls buyers ask about

Control	How we meet it	Status
5.19 to 5.22 Supplier relationships	Our own suppliers are few: AWS, for hosting and key management, and Google Workspace, for email; listed under NDA	Met
5.23 Cloud services	AWS Key Management Service (FIPS 140-3 hardware), encrypted storage and volumes, token-protected instance metadata	Met
5.24 to 5.28 Incident management	A written plan and a customer notification commitment	Planned
5.29, 5.30 Continuity	Your software keeps running without us: the licence works offline; source escrow on request	Met
5.34 Privacy and protection of personal information	The software sends no personal information to Senua AI	Met
5.35 Independent review	Penetration testing and certification	Planned

The other standards Standards Australia names

Standard	Where we stand
AS/NZS ISO/IEC 27002:2022, security controls	The control set mapped above
AS/NZS ISO/IEC 27005:2024, security risk	The risk method of our management system, with certification
AS 27701:2022, privacy information management	The software sends no personal information to Senua AI; your privacy controls stay in your hands
AS ISO/IEC 27035, incident management	With the incident plan
ISO/IEC 30111:2019, vulnerability handling	Fixes go to the root cause and remove the whole class of fault; the disclosure policy follows
ISO/IEC TR 6114:2023, security across the product life cycle	Requirements, design, review, signed release, tested removal
ISO/IEC 19772:2020, authenticated encryption	AES-GCM, one of its mechanisms, protects connections and the sealed software; AES-256-GCM protects everything stored since October 2026
ISO/IEC 9798-1:2010, entity authentication	Connections authenticate the server; releases and licences are signed
ISO/IEC 42001:2023 and AS ISO/IEC 23894:2023, AI	The software learns only from your own data, records the evidence behind every block, and blocks nothing until you allow it

About this datasheet

Senua AI's own mapping. It is not a certificate, and it implies no endorsement by Standards Australia or ISO. Planned items carry dates on the assurance roadmap, senuaai.com/technology/standards/roadmap/. Questions: sales@senuaai.com.