For procurement teams

For bank, fintech and government security reviews of Senua AI's cyber security software. The software runs on your own servers: your traffic, logs and everything it learns stay with you, Senua AI has no remote access, and the licence works offline. This datasheet sets out who is responsible for what, how the software fits APRA's CPS 234 and CPS 230 and the government frameworks, our answer to each of ASD's questions for buyers of software, and the dated steps still to come.

Shared responsibilities (ISM-1569)

Area	Senua AI	You
Software integrity	Builds, signs (ECDSA P-384, key in AWS KMS) and publishes each release; your installed verifier checks the next one before unpacking	Installs and upgrades; keeps the installed verifier
Flaws in our software	Finds, fixes and discloses them; fixes at no charge; tells affected customers	Applies releases on your patch timeframes
Host, operating system, network, HTTPS front end	Publishes host requirements and hardening guidance	Hardens, patches and runs them; backs them up
Accounts and console access	Enforces multi-factor sign-in for privileged accounts, lockout, password rules, roles and audit	Enrols people, sets roles, reviews the audit log
What the software learns	Encrypts it at rest under a key you control: AWS KMS, systemd credentials or your own key file	Holds the key; backs up, keeps or destroys the data
Logs and monitoring	Records every administrative action in a tamper-evident log; delivers events signed, by webhook, REST or email	Collects them into your SIEM and watches them
Licence	Issues a licence that verifies offline and never needs a connection to run	Keeps the licence file

Banks and fintech: APRA

Standard	What it asks of you	What we give you
CPS 234 Information Security	Assess the information security capability of any third party that manages your information assets; tell APRA within 72 hours of a material incident	We manage none of your information: your assessment is of the software and our supply chain, using these datasheets, the cryptographic register and the registry under NDA. From November 2026, we tell affected customers within 24 hours of confirming a flaw or incident
CPS 230 Operational Risk Management	For a material service provider: a formal agreement with access for you and APRA, subcontractors disclosed, data ownership, notification, continuity and exit	We sign those terms. Our subcontractors are AWS and Google, for our own hosted services only. Your data is in your environment. The software keeps running if we cannot, because the licence works offline; source escrow on request

Government

Framework	How it applies
PSPF 2025, Policy 6	Agencies put security terms into supplier contracts and see them applied; these datasheets and the terms we sign are written for that
IRAP	Assesses your system, with our software inside it; we give your assessor these datasheets and the registry under NDA
Hosting Certification Framework	Covers providers hosting government data; we host none

Framework	How it applies
DTA policy for the responsible use of AI	The software learns only from your own data, records the evidence behind every block, and blocks nothing until an administrator allows it

ASD's questions for buyers of software

From "Choosing secure and verifiable technologies" (ASD and partners, May 2024), question by question.

Question	Our answer
Has the manufacturer published threat models, a disclosure policy and CVEs?	The disclosure policy, security.txt and advisories with CVE numbers are on the roadmap below; our design and threat analysis can be reviewed under NDA
Have the organisation and product been assessed against standards? Independent or self? Date, version, frequency?	Self-assessed against ASD Essentials, the ISM of September 2026 and ISO/IEC 27001 Annex A, dated and reissued with each release; independent testing and certification are on the roadmap
Are all security features in the base product?	Yes. Multi-factor sign-in, audit, roles, encryption at rest and signed updates are in every edition
Are defaults set to the highest security? Is there a loosening guide?	Report only, nothing outbound, the engine on the local host; the hardening and loosening guide is on the roadmap
Are there default passwords? Is there MFA or SSO? Are configuration changes audited?	No default passwords. MFA required for administrators. Every setting change is audited. Single sign-on is on the roadmap
What encryption protects data at rest, in transit and in use?	Every algorithm is in the cryptographic register: TLS 1.3 in transit; 256-bit authenticated encryption at rest, under your key
What ICAM, SIEM and SOAR integration is there?	Local accounts with MFA; events by signed webhook, REST or email; a published event catalogue and a standard syslog format are on the roadmap
Is there a supply chain risk plan? Single-supplier reliance?	No third-party code in the engine or products beyond the standard C library. We build, sign and host on AWS; software you have installed keeps running without us or AWS
Is open-source software listed in an SBOM?	The only open-source component is the musl C library; a CycloneDX SBOM with each release is on the roadmap
Will the manufacturer collect data while you use the product? Where is data held?	No data is collected. Everything stays in your environment, in the region you choose
Is development secure by design, and attested against the ISM or SSDF?	Yes: written requirements and designs, review of every change, signed releases; our ISM self-assessment is published
What testing evidence is there?	Test suites run before every build; cryptography checked against published vectors; each release test-installed on a fresh host; the software runs on our own sites; independent penetration testing is on the roadmap
Does the manufacturer operate in high-risk regions?	No. Senua AI is an Australian company, developing in Australia; our demonstration and website forms run on AWS in Sydney
Is remote access by the manufacturer required? Is data retained by the manufacturer?	No remote access is required, and none exists. We retain none of your data
Are there change control processes?	Every change is registered with its checks before the code, reviewed and recorded
Does the product use open standards? Any lock-in?	TLS 1.3, FIPS and RFC algorithms, HTTP and JSON; what the software learns stays yours
Is there a policy for end of life and data disposal?	All data is in your environment; uninstall is tested with every release; the support and end-of-life policy is on the roadmap

The assurance roadmap

Step	What it gives you	Date
Disclosure policy and security.txt	A published way to report a flaw, response times, and advisories with CVE numbers	November 2026
Incident notification	Affected customers told within 24 hours of our confirming a flaw or incident	November 2026
Secret scanning	Every commit checked for keys and credentials, and refused if it holds one	November 2026
Software bill of materials	CycloneDX SBOM and build provenance with every release	December 2026
AI statement for each product	What it does and does not do, what it learns and from whose data, how a person stays in control	December 2026
Hardening guide and support policy	Every setting and its risk; supported releases and notice periods	December 2026
Independent penetration test	An accredited tester's report under NDA, then every six months	March 2027
Passkeys	Phishing-resistant sign-in to the console	March 2027
SIEM-ready events	A published event catalogue and a standard syslog format	March 2027
Single sign-on	OIDC and SAML, through your own identity provider	June 2027
ISO/IEC 27001 certification	Our information security management system certified by an accredited body	September 2027

About this datasheet

Senua AI's own answers, as shipped on the issue date. It is not legal advice and states no obligation of yours on APRA's or ASD's behalf; the standards' own text governs. The security review pack under NDA (the full cryptographic registry, what every connection negotiates, where our hosted services run): sales@senuaai.com.