The Information Security Manual

The controls of the Australian Signals Directorate's Information Security Manual (September 2026) that a buyer asks a software supplier about, with how Senua AI's software and practice meet each. Compliance with the ISM is judged for a whole system by an IRAP assessor; this datasheet is the supplier's evidence for that assessment. Control wording is ASD's, shortened but never changed in meaning.

Software development

Control	What it asks	How we meet it	Status
ISM-0400	Development, testing, staging and production environments are segregated	Builds on dedicated hosts; every release test-installed (install, upgrade, uninstall) on a fresh throwaway host before release	Met
ISM-2023, 2024, 1422, 1816	An authoritative source for software, used for all development, protected from unauthorised access and change	Private source repositories; every change reviewed and recorded	Met
ISM-2033, 2034	Security requirements documented; security design decisions documented and reviewed	Written requirements with acceptance tests; design notes written before code	Met
ISM-0401, 2042	Secure by Design and Secure by Default followed throughout	Every security feature in every edition; no default credentials; report-only default; engine on the local host	Met
ISM-2040	Secure programming practices for the chosen language	Senua AI's own language, with its written rules and lint gates	Met
ISM-1797	Installers, patches and updates digitally signed or given cryptographic checksums	ECDSA P-384 and SHA-384 by a key in AWS KMS (FIPS 140-3 HSM); SHA-256 manifests checked again at install	Met
ISM-1796	Executable content signed by a certificate with a verifiable chain of trust	Signed and verified against the release's pinned public key; a certificate chain beside it is planned	Partly met
ISM-2044	No default credentials; any credentials created at first install by the installing organisation	A random single-use first credential, disclosed only on your host at first run	Met
ISM-2048	Non-administrative users cannot alter their own permissions	Capabilities enforced by the engine	Met
ISM-2051, 2052	Enough event logs to detect security events; sensitive data in logs protected	Tamper-evident audit log; secrets kept out of evidence records	Met
ISM-2026, 2027, 2029	Imported artefacts scanned and verified; third-party libraries only from trustworthy sources	No third-party library is imported into the engine or products; the only outside component is the standard C library (musl), statically linked	Met
ISM-2154	Dependencies pinned to approved versions in source code	No third-party packages to pin; compiler and runtime in the same source at a recorded version	Met
ISM-2032	Automated testing completes without warnings or errors before artefacts are built	The build gate lints every product source and runs every product test suite; the first failure stops the build	Met
ISM-2155	Reproducible builds that let anyone verify a release came from its stated source	The compiler rebuilds itself byte for byte; release objects compared byte for byte; a published rebuild procedure is planned	Partly met

Control	What it asks	How we meet it	Status
ISM-2083	A cryptographic bill of materials made available to consumers	The full cryptographic registry, under NDA; the public register at senuaai.com/technology/security/	Met
ISM-1730, 2056	A software bill of materials and build provenance made available to consumers	With each release	Planned
ISM-1817, 1818	Clients of network APIs authenticated and authorised	Every console and API route requires a session or an API key, checked by the engine	Met
ISM-1240, 2016	Input validated and sanitised	Request fields checked against declared rules before use	Met
ISM-2060, 2061, 2062	Code and peer review; unit and integration tests, positive and negative	Every change reviewed against a written gate and recorded; test suites; cryptography against published test vectors and an independent implementation	Met
ISM-1616, 1755, 1756, 1717, 1908	A vulnerability disclosure program, policy, procedures and security.txt; public disclosure with CWE	Under the disclosure policy	Planned
ISM-1909	Root cause analysis; whole classes of vulnerability remediated	Our practice: a fault class is fixed wherever it occurs	Met
ISM-2030	Commits scanned for credentials, keys and secrets, and blocked	Secret scanning at every commit	Planned
ISM-1798, 2053	A hardening or loosening guide; end-of-life procedures, including removal and data destruction	Uninstall tested with every release; the guide and the support policy are planned	Partly met
ISM-2063, 2065, 2066	Session cookies HttpOnly, Secure and SameSite; random opaque tokens of at least 128 bits; sessions managed server side	HttpOnly and SameSite=Strict; 256-bit random tokens held by the engine and stored only as hashes; the Secure flag is planned	Partly met
ISM-1424	Content-Security-Policy, HSTS and X-Frame-Options	The console sends a content security policy and X-Frame-Options: DENY; HSTS is set at your HTTPS front end	Met, with yours

Artificial intelligence

Control	What it asks	How we meet it	Status
ISM-2113	AI applications require human approval before sensitive or high-impact actions	Report only by default; blocking is switched on by an administrator, and the change is audited	Met
ISM-2103	Organisational data not used for training without informed, explicit consent	The software learns only inside your install; nothing reaches Senua AI	Met
ISM-2072, 2086	Models in a non-executable format; their source and integrity verified	What the software learns is data in an encrypted, authenticated store, with signed batches	Met
ISM-2156 to 2159, 1924	Controls for agentic and generative AI applications	Not applicable: the software calls no tools, generates no text and takes no instructions from content	Not applicable

System access

Control	What it asks	How we meet it	Status
ISM-1173	MFA for privileged human users	Required: a privileged account without a second factor can do nothing but enrol one; enforced by the engine	Met

Control	What it asks	How we meet it	Status
ISM-0974, 1401	MFA for unprivileged users; something you have with something you know	Available to every account: password with an authenticator app	Met
ISM-1682, 1872	Phishing-resistant MFA	Passkeys	Planned
ISM-1403	Lockout within a maximum of five failed attempts	Locked at the fifth failure in a 15-minute window	Met
ISM-1227	Credentials randomly generated	The first credential is random	Met

Procurement and outsourcing (what you apply to us)

Control	What it asks	How we meet it	Status
ISM-1568, 1882, 1632	Suppliers committed to security and transparency, with a track record	Public standards pages and cryptographic register; the full registry under NDA	Met
ISM-1569	A shared responsibility model, documented and shared	Published in the procurement datasheet	Met
ISM-1790, 1791, 1792	Delivery that keeps integrity; integrity and authenticity checked at acceptance	Signed releases, verified before unpacking	Met
ISM-1073, 2124, 2125, 1576	Service provider access controlled, restricted and independently logged	Not applicable by design: Senua AI has no access to an installed system	Not applicable
ISM-1572, 1573, 1574	Data regions, log access and portable data in contracts	All data stays in your environment, in a store you control	Met
ISM-1793, 1570	IRAP assessment of managed and cloud services	Not applicable: the software is not a managed or cloud service; your IRAP assessment covers it inside your system	Not applicable

Cryptography

ISM-1917 and ISM-2073, and the status of every algorithm, are in the cryptographic register datasheet and at senuaai.com/technology/security/.

About this datasheet

Senua AI's own assessment against the ISM of September 2026 (catalogue release v2026.09.4). It is not an IRAP assessment or an ASD endorsement. Planned items carry dates on the assurance roadmap, senuaai.com/technology/standards/roadmap/. Questions: sales@senuaai.com.