Client IP Protection & Data Security

Written into the contract — not left as a promise

Since 2001, Shinetech Software has maintained a zero IP-dispute record across its client base.

900+ AU Clients | ISO 27001 Certified | Cyber Essentials Plus Certified

We only provide technology services — we don't build our own products. That business model alone removes any incentive to compete with clients or repurpose their work; your data sovereignty stays with you, start to finish. Below are the concrete mechanisms behind both commitments.

1. Protection Starts From the First Conversation

Before any contract is signed, Shinetech signs an NDA first — the business ideas and logic a prospective client describes are legally protected before the contract even exists; Shinetech staff are prohibited from disclosing that information outside the company or using it for their own purposes.

2. Ownership: Locked in Writing, Not Assumed by Default

Ownership of all project deliverables — including source code, software architecture, technical documentation, and any trade secrets developed during the project — is expressly assigned to the client under the Master Service Agreement (MSA) and Statement of Work (SOW), except for pre-existing rights in third-party open-source/commercial code and Shinetech's general-purpose technical components.

One note: in many jurisdictions, code copyright defaults to the developer, not the client. Ownership “by the client” is not automatic — it has to be locked in with precise contract language. Shinetech has already built this into its standard contract templates, so clients do not need to negotiate for it themselves.

If a project involves subcontracting, subcontractors must sign IP protection and confidentiality agreements of equal rigor — responsibility does not dilute as the outsourcing chain lengthens.

3. Code Control: Stays in the Client's Account by Default

- Code is hosted by default on the platform the client designates (GitHub Enterprise, GitLab, etc.); Shinetech receives only the minimum access needed to collaborate.

Hosting on Shinetech's own repositories requires the client's written consent, with least-privilege access and full audit trails.

- Outside milestone-based delivery contracts, development teams typically commit the latest code daily, so clients can review or pull the complete source code at any time — no need to wait for a delivery milestone.
- At the end of each phase or project, Shinetech delivers the complete source code, build scripts, and necessary technical documentation so clients can build and deploy independently, without depending on Shinetech.
- Commit history and access logs are fully retained, keeping development progress traceable throughout.

4. People: Protecting IP and Data Ultimately Comes Down to People

- Background checks on hiring (identity, education, work history); staff sign a Confidentiality Agreement[1] and an IP Protection & Data Security Commitment[2], with obligations that survive their departure.
- Least-privilege access management, plus a mandatory asset handover audit upon departure to ensure no client code or data is retained.

Average staff turnover has stayed below 5% over the past five years. Engineers who understand a client's business logic stay on the project, instead of rotating out and starting handover from zero.

5. Production Environment: Data Sovereignty Stays With the Client Throughout

Shinetech does not host production environments or sell SaaS products. Whether a client deploys on AWS, Azure, GCP, or its own data center, control, access, and audit rights over the infrastructure always remain with the client.

- Shinetech never holds or hosts client production data; it always remains within the client's sovereign control.
- For operations support, Shinetech staff log in only through secure remote access methods the client authorizes (VPN, bastion host, jump server); Shinetech never

[1] Covers all information the client shares with Shinetech, plus any information arising during the project. Confidentiality applies by default, except for information that is already public.

[2] Covers two areas: IP protection — safeguarding the client's proprietary information and all deliverables produced while working for the client; and data security — ensuring data is handled lawfully and in compliance with applicable regulations.

migrates data or systems into its own environment. Any data backup work is performed only in environments the client has authorized in writing.

- Access is granted by the client under the principle of least privilege; where a bastion host is available, Shinetech's operations can be fully screen-recorded for an audit trail.

6. Cross-Border Compliance: Synthetic Data by Default, Clear Ownership of Responsibility

Shinetech's China-based development and testing teams use “synthetic data” by default and never touch a client's real customer information. Synthetic data is programmatically or manually generated, non-reversible, and contains no real personal information belonging to any client; it is used for day-to-day feature development, unit testing, and load testing. Masked data — or, in rare, necessary cases, real data — is used only with the client's written consent, always under full audit.

For clients subject to strict data protection regimes such as GDPR and CCPA, Shinetech's UK, US, and Australian subsidiaries act as local data processors, bearing responsibility under local law and maintaining a clear separation of duties from the China-based technical team. If accessing personal data within China is genuinely necessary in a specific case, Shinetech can put in place and execute the appropriate cross-border transfer mechanism.

Shinetech's coding standards prohibit hardcoding any personal information — names, emails, phone numbers, and the like are always retrieved on demand from a database or configuration center. As a result, the code itself contains no personal data, and where the code is stored is purely an asset-management decision, not a cross-border data compliance issue.

7. Independent Certification: Verified by Third Parties, Not Self-Declared

At the technical level: codebases, servers, and network environments are physically and logically isolated between client projects; codebase access uses multi-factor authentication (MFA) with full logging; development, testing, and production environments are strictly segregated; and strong encryption protects data in transit and at rest.

In the event of a security incident: Shinetech follows a defined incident response plan (severity classification, response process, division of responsibility), notifying the client and cooperating with the investigation within the agreed timeframe — not improvising after the fact.

Certification / Standard	Scope	What It Verifies
ISO 27001:2022	Beijing HQ (certified)	Full lifecycle management of

		information asset identification, risk assessment, and continuous improvement
Cyber Essentials Plus	UK subsidiary (certified)	Endorsed by the UK government (NCSC); independent penetration testing verifies perimeter defense capability

Client Concerns at a Glance

Client Concern	Shinetech's Arrangement
Who owns the code once the project is done?	The MSA/SOW state in writing that the client retains 100% ownership.
Could the code get reused on another project?	Technical isolation between client projects; code sits in the client's own repository by default; staff sign a Confidentiality Agreement and an IP Protection & Data Security Commitment as a backstop.
Where is my production data?	Always in the client's own production environment; Shinetech does not host it or back it up to its own environment.
Does the China-based team ever see my real customer data?	Synthetic data by default; where compliance requires it, an overseas subsidiary takes on local data processor responsibility.
Could a departing engineer take something with them?	Mandatory asset audit on departure, confidentiality obligations remain in force, and team turnover is below 5%.
Who has verified the word “secure”?	ISO 27001 and Cyber Essentials Plus are both third-party audited and certified — not self-declared.

If you're evaluating a software development partner for your next project, we'd welcome the conversation. Contact us: salesau@shinetechsoftware.com or +61 (0)424 188 308.

This document is for informational reference only. It does not constitute legal, contractual, or professional advice, and does not modify, supplement, or replace the terms of any agreement signed by the parties. Execution of specific projects is governed by the agreement signed by both parties.