INDIALAW

Trade Secrets & Confidential Information

Trade Secrets Law Firm in India for Confidentiality, Licensing, and Enforcement

PRACTICE PROFILE • MAY 2026

Overview

Our Trade Secrets & Confidential Information practice helps businesses protect their proprietary information and know-how through comprehensive legal strategies. We develop tailored protection programs that identify, secure, and enforce rights in confidential business information, complementing formal IP registrations with robust trade secret protection to maintain competitive advantages.

Our Services

Trade Secret Protection Programs

- Development of information classification systems
- Protection policies and procedures
- Employee training programs
- Security protocol implementation

Confidentiality Agreements

- Non-disclosure agreement drafting
- Confidentiality clause development
- Employee confidentiality obligations
- Third-party information exchange frameworks

Technology Transfer

- Know-how licensing arrangements
- Trade secret commercialization
- Technology transfer agreements
- International know-how protection

Employee-Related Measures

- Employment contract confidentiality provisions
- Exit interview protocols
- Post-employment restrictions
- Inevitable disclosure doctrine applications

Enforcement Actions

- Trade secret litigation
- Breach of confidence actions
- Emergency injunctive relief
- Damage assessment and recovery

Digital Security

- Data security legal frameworks
- Cybersecurity compliance
- Digital information protection measures
- Cloud storage security protocols

Supply Chain Protection

- Vendor confidentiality management
- Manufacturing partner restrictions
- Distribution channel protection
- International supply chain security

Key Professionals

Shiju P V
Managing Partner

Vinod P.V.
Senior Partner

Frequently Asked Questions

Q1 **What does a trade secrets and confidential information practice cover?**

It covers identifying, classifying, and protecting proprietary business information such as formulas, processes, customer data, and know-how. This includes drafting confidentiality agreements, building internal security protocols, managing technology transfers, and enforcing rights through litigation or injunctive relief when breaches occur.

Q2 **When should a business invest in a formal trade secret protection program?**

Ideally before a triggering event, not after. Key moments include onboarding senior hires, engaging third-party vendors, entering joint ventures, or expanding into new markets. A structured program is also critical when employees with access to sensitive information are exiting to competitors.

Q3 **Which Indian laws govern trade secret protection and confidential information?**

India has no standalone trade secret statute. Protection relies on contract law, the Indian Contract Act 1872, the IT Act 2000, the DPDP Act 2023 for personal data, and common law principles of breach of confidence. Courts have consistently upheld contractual confidentiality obligations and granted injunctions in trade secret disputes.

Q4 **How long does it take to set up a trade secret protection framework?**

A comprehensive program typically takes 8 to 16 weeks, depending on the organisation's size and complexity. Key cost drivers include the scope of the information audit, number of employee and vendor agreements requiring drafting or revision, and the level of security protocol integration needed across business units.

Q5 **What documents or information should a client prepare before engaging counsel?**

Clients should gather existing employment contracts, NDAs, vendor agreements, IT security policies, and any internal information classification records. An organisational chart showing who accesses sensitive data, along with details of any known or suspected breaches, helps counsel assess risk and prioritise action areas.

Q6 **What is the most common mistake companies make with trade secret protection?**

Relying solely on NDAs without implementing internal safeguards. Indian courts assess whether the information holder took reasonable steps to maintain secrecy. Without access controls, classification systems, and documented security measures, enforcing rights in a breach of confidence action becomes significantly harder.

Related Practice Areas

Intellectual Property Disputes