Employee IP Training Module (India)

Structured training content for employee IP awareness at onboarding and annually

HOW TO USE THIS TEMPLATE	
1.	This document: Employee IP Training Module (India).
2.	Fill all bracketed fields before use.
3.	Template only — not a substitute for qualified legal advice.

MODULE 1 — WHAT IS IP AND WHY IT MATTERS HERE

Our IP Is Our Business. The software we build, the brand we have created, the trade secrets we protect, and the data we compile represent a significant portion of this company's commercial value. Protecting IP protects your job, your equity, and the company's future. An IP breach can reduce the company's value by millions in minutes.

Types of IP at This Company. Software and algorithms (copyright and potentially patents); brand and trademarks (registered trademarks and goodwill); trade secrets (our methods, processes, client data, and know-how); and creative content (designs, marketing materials, written content). Each type has different rules and protections.

Consequences of IP Breaches. Employment termination; personal civil liability for damages; criminal prosecution (copyright theft and trade secret theft can lead to imprisonment under Indian law); reputational damage affecting future career; and significant financial harm to colleagues and investors.

MODULE 2 — OWNERSHIP AND PERSONAL PROJECTS

The Company Owns What You Create at Work. Under Section 17 of the Copyright Act 1957, works created by employees in the course of employment are owned by the employer. This applies even if you work from home on your own device. 'In the course of employment' means: during working hours; using company resources; in furtherance of your job role; or at the company's direction.

Your Personal Projects — The Rules. You may maintain personal projects created entirely outside working hours, using no company resources, and unrelated to the company's business domain. If any doubt exists whether a personal project conflicts with your employment obligations — disclose it to your manager before starting. Keeping it undisclosed and then using it in your work creates serious legal complications.

Pre-Existing IP Disclosure. Any IP you created before joining that is relevant to your work here must be disclosed. We will agree in writing what, if anything, is assigned to the company. Disclose at onboarding — do not wait for a conflict to emerge.

MODULE 3 — CONFIDENTIALITY AND TRADE SECRETS

What Is Confidential. Everything non-public. This includes: source code and technical architecture; customer names, contacts, and commercial terms; product roadmap and features in development; financial data and fundraising discussions; employee compensation and performance data; and any business strategy not publicly announced.

Confidentiality Rules in Practice. Use only company-approved tools for company work. Do not save confidential data to personal cloud storage (personal Google Drive, Dropbox, iCloud). Do not share confidential information over personal messaging apps. Use the company VPN when accessing sensitive data remotely.

After You Leave. Your confidentiality obligations do not end when your employment ends. The obligation to protect genuine trade secrets is legally binding and indefinite. You may not take copies of company data when you leave. You may not share what you learned here with a new employer if it includes the company's trade secrets.

MODULE 4 — PRACTICAL RULES

Open-Source Rule. Never add an open-source component to the company's codebase without checking the licence first. Permissive licence (MIT, Apache 2.0, BSD): generally safe. Copyleft (GPL, AGPL, SSPL): get IP Manager approval before adding. One wrong GPL dependency can force the entire codebase to be open-sourced.

AI Tools Rule. Never enter company source code, customer data, trade secrets, or confidential business information into any AI tool that may use inputs for model training. Check the enterprise terms of any AI tool before using it for company work.

Reporting Obligation. If you discover suspected IP theft — a colleague bulk-downloading code, a competitor using our brand, our trade secrets appearing elsewhere — report immediately to the IP Manager. You will be protected from retaliation for good-faith reports.

Contractor and Partner Interactions. Do not share technical details, roadmap information, or confidential pricing with vendors or partners beyond what is strictly necessary, and only after they have signed an NDA.

IMPORTANT NOTE

Working template for Employee IP Training Module (India). Verify requirements with a qualified IP advocate.

CASE STUDIES — WHAT IP BREACHES LOOK LIKE AND THEIR CONSEQUENCES

Real-world context makes IP training stick. The following case study scenarios illustrate common IP risks and their consequences, without referencing any specific companies. Case Study 1 — The Departing Developer: A senior backend developer resigns to join a competitor. On their last day, they email themselves a copy of the core authentication library they wrote, intending to use it as a reference

in their new role. What happens: the departure triggers a routine forensic review; the email is discovered; the company sends a formal demand for deletion and a written undertaking; the developer's new employer is notified; and the developer faces personal civil liability for copyright infringement and breach of employment contract. Lesson: all company code is company property. Taking any copy on

departure, for any reason, is a breach of the employment agreement. Case Study 2 — The Well-Intentioned Contributor: A frontend developer at the company, in their personal time, contributes a bug fix to a popular open-source charting library. The bug fix is derived from code they wrote at work for a similar charting feature in the company's product. What happens: the contribution is made under MI

T licence, making it publicly available. A competitor uses it in their product. The company's IP advantage in the charting feature is permanently lost. Lesson: any contribution derived from company code requires IP Manager approval — even small bug fixes. Personal time is not the relevant test; the origin of the code is. Case Study 3 — The Helpful Employee: A junior sales team member, wanting to h

elp close a prospect, shares a detailed technical architecture diagram with the prospect before an NDA was signed. What happens: the prospect, who was also evaluating a competitor, passes the architecture information to the competitor. The competitor launches a similar feature 3 months ahead of the company. Lesson: no technical information, pricing data, or internal presentations should be shared

externally without confirming that an NDA is in place and confirming with the manager that the sharing is appropriate.

ADDITIONAL COMPLIANCE GUIDANCE AND BEST PRACTICES

ADDITIONAL GUIDANCE ON COMPLIANCE AND BEST PRACTICES. Indian IP law continues to evolve rapidly, with the Patent Office, Trade Marks Registry, and Copyright Office all implementing digital transformation initiatives that affect how IP is filed, prosecuted, and enforced. The Patents Amendment Rules 2024 introduced new provisions for startup fee concessions and updated the examination procedure timelines. The Trade Marks Act 1999 has been interpreted by courts in a growing body of decisions that clarify how confusion is assessed, how well-known

marks are recognised, and how bad faith is established. The DPDP Act 2023 has implications for IP-linked customer data and product development processes. For each IP action described in this document, the Company should consult a qualified IP advocate licensed to practice before the Indian Patent Office and Trade Marks Registry. IP advocates combine technical expertise with legal training specific to Indian IP law. When selecting an IP advocate, assess: their specific experience in your technology sector or product category;

their track record at the relevant Patent Office branch or Trade Marks Registry; and their ability to coordinate international filings through their network of foreign associates. The IP Manager should maintain a master calendar tracking all IP filing deadlines, prosecution response deadlines, renewal dates, and opposition window close dates. IP deadlines are typically non-extendable and missing them can result in permanent loss of rights. Use a dedicated IP management tool or a carefully maintained calendar system with triple-reminder alerts. Document

all IP decisions and the reasoning behind them. When the Company decides not to file a patent application for a particular technology, document the decision and reasoning. When a trademark opposition is decided not to pursue, document the decision. This decision trail is important for investor due diligence, management continuity, and defence of subsequent IP disputes. Build a quarterly IP Committee meeting cadence: the IP Manager, CTO or Head of Product, CFO, and CEO should review IP programme status, upcoming

decisions, and strategic IP priorities every quarter. This keeps IP on the leadership agenda and ensures that commercial and technical strategy is aligned with IP investment decisions. The IP Committee meeting should produce a brief written record of decisions taken and actions assigned. International IP coordination requires proactive management of priority deadlines. The Paris Convention priority period of 12 months for patents and 6 months for trademarks and designs starts from the Indian filing date. If international protection is planned,

calendar these priority deadlines immediately on the Indian filing date. The cost of filing internationally increases significantly if priority is not claimed because prior art in the intervening period may destroy novelty. Budget for professional indemnity insurance for the IP function. As IP becomes a larger component of the Company's value and IP decisions involve significant financial stakes, the IP Manager and the Company's IP counsel should be appropriately insured against errors and omissions. Review the IP programme's documentation quality

annually. The best IP strategy is undermined by poor documentation. Every IP right should have a complete file: the registration or application document, all prosecution history, all renewal receipts, and all related agreements. Files should be backed up in at least two locations and access-controlled to prevent inadvertent deletion. Template only. Not legal advice. Consult a qualified IP advocate for all decisions affecting the Company's intellectual property rights.