Whistleblower and IP Theft Reporting Policy (India)

Policy enabling employees to confidentially report IP theft, misappropriation, and policy violations

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

1. PURPOSE AND IMPORTANCE

Why Internal IP Theft Is the Biggest Risk. The most common source of IP theft for Indian startups is internal — by departing employees, disgruntled current employees, or contractors with system access. External hacking receives more attention, but insider threats are more frequent and often more damaging because insiders have legitimate access to the most sensitive systems.

The Role of the Whistleblower Channel. A safe, confidential reporting channel enables employees who witness potential IP theft to report without fear of retaliation. Colleagues are often the first to notice unusual behaviour — bulk downloads, odd-hours access, unusual printing — and they have the contextual knowledge to interpret that behaviour as suspicious.

Legal Framework. India's Whistle Blowers Protection Act 2014 covers public sector disclosures. For private companies, whistleblower protection is contractual — this Policy creates a contractual obligation not to retaliate against reporters making good-faith reports.

2. WHAT TO REPORT AND HOW

Report immediately: Colleagues downloading or emailing bulk files to personal accounts; accessing systems outside their normal scope at odd hours or before departure; Company trade secrets or source code appearing in competitor products; contractors using Company IP beyond their contract scope; visitors who appear to be copying confidential information.

How to Report. Confidential: Email ipsecurity@yourcompany.com (monitored by IP Manager only). Anonymous: web form at [your intranet URL] if you prefer not to identify yourself. Both channels are treated with strict confidentiality. Include: description of what you observed; when and where; who is involved; any evidence you can document without alerting the subject.

What NOT to Do. Do not confront the subject yourself — this may alert them to destroy evidence. Do not report to the subject's manager first — their manager may be involved or may tip them off. Do not post about it on any platform.

3. INVESTIGATION PROCESS

Initial Triage (within 24 hours). IP Manager acknowledges receipt; assesses credibility and urgency; determines what evidence can be preserved immediately without alerting the subject.

Evidence Preservation First. IT secures server logs, access records, email metadata, and system audit trails before any investigation contact with the alleged subject. This preserves forensic evidence that would otherwise be lost if the subject is alerted.

Confidentiality. The reporter's identity is kept strictly confidential throughout. The IP Manager, one senior HR representative, and legal counsel are the only parties with access to investigation details. The subject is not informed until the investigation is complete.

Outcomes. If evidence is sufficient: disciplinary action up to and including termination; civil action for damages; criminal complaint if appropriate. If evidence is insufficient: investigation closed; file retained confidentially.

4. ANTI-RETALIATION PROTECTION

The Guarantee. Any employee who takes adverse action against a good-faith reporter — including demotion, exclusion, harassment, negative performance review, or any other adverse employment action connected to the report — will face immediate disciplinary action up to and including termination.

This Guarantee Applies Regardless of Outcome. Even if the investigation concludes that the reported behaviour did not constitute IP theft, the reporter who made a good-faith report is protected. Retaliation against a reporter who turned out to be mistaken is treated identically to retaliation against a reporter whose report was substantiated.

Encouraging a Reporting Culture. IP protection depends on a culture where everyone feels responsible for protecting the company's assets. Make reporting easy and safe. Acknowledge reporters (confidentially) that their report has been received and is being investigated. Follow up with reporters (without disclosing investigation details) when the investigation is resolved.

Annual Communication. Remind all employees annually: of the reporting channel; of the anti-retaliation guarantee; and of recent examples (anonymised) of IP protection actions taken. This communication reinforces that the policy is active, not theoretical.

IMPORTANT NOTE

Working template for Whistleblower and IP Theft Reporting Policy (India). Verify requirements with a qualified IP advocate.

DIGITAL FORENSICS AND EVIDENCE PRESERVATION ON IP THEFT DISCOVERY

When an IP theft report is received or an incident is suspected, the first 24 hours are critical for evidence preservation. Digital forensic evidence degrades, is overwritten, or can be deliberately destroyed quickly — a structured immediate response protocol is essential. The Evidence Preservation Protocol: within the first hour of a credible IP theft report being received: (1) The IP Manager imm

ediately contacts the IT Manager (or IT security lead) by phone, not email — internal email systems may be accessible to the suspected person. (2) The IT Manager immediately preserves: server-side email logs for the suspected person for the past 90 days; cloud storage access logs (Google Drive, OneDrive, Dropbox business accounts) showing file access, download, and sharing activity; git commit and

repository access logs for the past 90 days; VPN access logs showing remote access from non-company devices; and all system and application access logs for the past 30 days. (3) The suspected person's company accounts (email, Slack, Jira, CRM) are placed in a legal hold — all data preservation is enabled, all deletion is disabled. This must be done without notifying the account holder. (4) If the

suspected person is still active in the company, access to the most sensitive systems (production databases, IP repositories, customer data) is restricted immediately under the pretext of a routine security review. (5) The IT Manager creates a forensic image of the suspected person's company laptop or desktop (if in the office) or issues a formal request for device surrender (if remote). Device i

maging should be conducted by a qualified forensic professional using write-blockers to ensure the forensic image is admissible as evidence. Legal hold procedures: establish a formal legal hold policy that specifies: who may authorise a legal hold; what systems are subject to hold; the procedure for notifying custodians (in IP theft cases, notification of the suspected person is deferred until inv

estigation is complete); and how long holds are maintained. Document every step of the evidence preservation process with timestamps — this chain of custody documentation is critical if criminal charges are pursued.

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.