Software Escrow Agreement (India)

Agreement for holding source code in escrow for release on defined trigger events

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

1. PURPOSE AND COMMERCIAL CONTEXT

What Is Software Escrow. A software escrow arrangement involves a neutral third-party escrow agent holding source code and technical materials for a software product. The deposit is held in confidence and released to the licensee only on defined release conditions — typically events that prevent the licensor from continuing to support the software.

Why Licensees Need Escrow. A software licensee relying on proprietary software for mission-critical operations faces business continuity risk if the licensor becomes insolvent, is acquired and the product discontinued, or ceases maintenance. Escrow gives the licensee a right to access source code in these scenarios — enabling them to maintain the software themselves.

Why Licensors Should Offer Escrow. Offering escrow: builds licensee confidence and can enable enterprise sales; is required by many large enterprise and government customers; demonstrates maturity and long-term commitment; and is less burdensome than the commercial cost of losing deals due to its absence.

2. KEY AGREEMENT PROVISIONS

Deposit Obligations. Depositor must provide: complete current source code for all components; build instructions and development environment specifications; all third-party libraries and components (or instructions for obtaining them); database schemas and data dictionaries; API documentation; deployment and configuration documentation; and test suites. Update deposit within 30 days of each material software release.

Verification Services. Escrow services offer technical verification — an independent technical expert reviews the deposit to confirm it is: complete (all components present); compilable (can be built into working software); and accurate (matches the production version). Include an annual verification schedule for Tier 1 critical software.

Release Conditions — Define Precisely. Classic release conditions: insolvency or cessation of trading by the licensor; failure to provide contracted maintenance within 90 days of written notice; material breach of the licence agreement not remedied within the cure period; and acquisition followed by material change or discontinuation of the software. Ambiguous release conditions are the most common cause of disputes.

Post-Release Obligations. Once released: the licensee may use the source code only for their own internal operational use; not for redistribution, sublicensing, or creating derivative products; and subject to confidentiality obligations. The licensor retains all copyright in the source code — release is a licence to use, not an assignment.

3. CLOUD AND SAAS CONSIDERATIONS

Limitations of Traditional Escrow for SaaS. Source code alone may be insufficient for SaaS products. The licensee would also need: cloud infrastructure setup; database and customer data migration; API keys and third-party service accounts; and technical staff to operate the service. Full reconstitution from source code alone may be prohibitive.

Cloud Escrow Solutions. Modern providers offer: continuous cloud environment snapshots; direct access to a replicated cloud environment on release; and data escrow covering the licensee's data stored in the SaaS platform. Evaluate cloud escrow for mission-critical SaaS products.

Continuous vs Periodic Escrow. Traditional periodic deposits (monthly or on release) may be significantly out of date when needed. Continuous escrow using automated build pipelines keeps the deposit current. For rapidly evolving software, continuous escrow provides substantially stronger protection.

4. NEGOTIATING AND SELECTING PROVIDERS

Licensor Perspective. When agreeing to escrow: ensure release conditions are narrowly defined; include confidentiality obligations on the escrow agent and the licensee for released materials; confirm released materials may only be used for the licensee's own internal use, not redistributed; and verify the escrow agent is genuinely independent.

Licensee Perspective. When evaluating a proposed escrow: verify the escrow agent is independent (not affiliated with the licensor); confirm the deposit is verified and current; ensure release conditions cover realistic risk scenarios; and confirm technical capability to use the source code if released.

Provider Selection in India. Escrow providers active in India: international providers (Escode NCC Group, Iron Mountain Escrow, SES Software Escrow Services) operating through Indian partners; and domestic providers. Compare: independence; verification capabilities; data sovereignty (where is the deposit stored?); and the release process timeline.

IMPORTANT NOTE

Working template for Software Escrow Agreement (India). Verify requirements with a qualified IP advocate.

INDIAN DATA LOCALISATION AND ESCROW COMPLIANCE

For Indian companies providing software to government, financial sector, and healthcare customers, data localisation requirements under Indian law create additional dimensions for software escrow arrangements. The Digital Personal Data Protection Act 2023 and sectoral regulations (RBI guidelines, SEBI guidelines, IRDAI guidelines, and NHA health data guidelines) require that certain categories of

sensitive personal and sectoral data be stored within India. For software escrow serving Indian regulated-sector customers: (1) The escrow deposit must be stored within India for regulated-sector licences where Indian data localisation applies. International escrow providers (who typically store in UK, US, or EU datacentres) may need to establish Indian storage arrangements to comply. Confirm the

escrow provider's India data centre capability. (2) Cloud escrow for regulated-sector SaaS products must comply with the RBI's outsourcing and cloud guidelines, which require the regulator's prior approval for cloud arrangements involving critical systems. Factor regulatory approval timelines into the escrow implementation plan. (3) Source code containing cryptographic components may be subject to

export control restrictions under India's SCOMET (Special Chemicals, Organisms, Materials, Equipment and Technologies) list and the Wassenaar Arrangement. Consult your export control counsel before depositing cryptographic source code with an international escrow provider. Technology transfer implications: in some cross-border software licensing arrangements, the escrow release to the licensee co

uld constitute a technology transfer requiring prior approval under FEMA (Foreign Exchange Management Act) regulations. If the software embodying significant proprietary technology will be released to a foreign licensee under the escrow, obtain FEMA advice on the applicable approvals before the release trigger is exercised. The escrow agreement should specify that any technology transfer regulator

y requirements will be met before release is effected.

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.