Confidentiality During and After Employment (India)

by Ayushi Singh, Anmol Suhane, Sayantani Saha, Soumit Nikhra, and Vikram Shroff, *AZB & Partners*

Practice notes | Law stated as at 01-Mar-2025 | India

A Practice Note on the issues arising in relation to confidentiality both during employment and after termination in India. This Note addresses what duties in relation to confidentiality are provided by law and how the employer can protect their confidential information, including drafting guidance for a confidentiality clause in their employment contracts. It also considers the law relating to whistleblowing in India.

Information is a key asset of most businesses. Many employees may have access to or create information and acquire valuable knowledge while working for their employer. Employers will want to ensure that they protect this information to the fullest extent possible to avoid any misuse by an employee that could dilute the value of this important asset.

While many jurisdictions have laws in place that may protect an employer's confidential information during and after employment, employers may be able to take steps, such as entering into a confidentiality restriction in their employment contracts with employees, to prevent employees making use of the information either for themselves or for a third party especially if they are a competitor.

This Practice Note explains:

- What duties in relation to confidential information can be implied by law.
- What information is considered confidential.
- How the employer can protect confidential information using a clause in the employee's employment contract.
- What remedies are available to an employer where the employee had made unauthorised use or disclosure of the employer's confidential information.

Confidentiality Protection in Employment

Confidentiality Obligations During Employment

In India, there is no specific statute that places a duty on employees to protect an employer's confidential information. However, Indian courts recognise the employee's implied obligation to protect an employer's confidential information (*John Richard Brady & Ors v Chemical Process Equipment P Ltd & Anr (AIR 1987 Delhi 372)*).

Indian courts recognise that employees have an implied duty to protect their employer's confidential information, based on common law principles. In the case of *Bombay Dyeing and Manufacturing Co. Lt. v Mehar Karan Singh (2010 (112) BomLR 375)*, the Bombay High Court held that an employee has an implied duty to safeguard the confidential information of the employer. Further, in their judgments, Indian courts have cited the broad principle of equity, which states that a person who receives information in confidence should not be allowed to unfairly exploit it (reiterated in *Fairfest Media Ltd v Ite Group Plc (2015 SCC OnLine Cal 23)*).

Additionally, there are state laws in certain states that consider the unauthorised disclosure of confidential information (obtained during employment) to third parties as misconduct. In these states, employers may take disciplinary action against employees who disclose confidential information to third parties during their employment, including terminating their employment. For example, the model standing orders (in states such as Maharashtra (Mumbai), Karnataka (Bangalore), Haryana (Gurgaon), and Telangana (Hyderabad)) outlined under *The Industrial Establishment (Standing Orders) Act, 1946* (Standing Orders Act) classify the unauthorised disclosure of an employer's confidential information related to the establishment's processes, which an employee may have access to during the course of their work, as misconduct.

A conciliation officer investigating a dispute under the Industrial Disputes Act, 1947, is bound by confidentiality obligations in respect of matters disclosed to them in the course of their employment. Further, the *Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013* (PoSH Act) prohibits the publication of information related to the identity and addresses of the aggrieved woman, respondent, and witnesses involved in conciliation or inquiry proceedings resulting from a sexual harassment complaint under the PoSH Act.

Employees of listed companies and individuals with access to any unpublished price sensitive information of listed companies must keep such information confidential pursuant to Securities and Exchange Board of India (Prohibition of Insider Trading) Regulations, 2015.

Also, employers include terms on confidentiality obligations in employment contracts and policies, and a breach of these obligations may constitute valid grounds for terminating employment, provided the necessary procedures are followed.

Confidentiality Obligations After Termination of Employment

Following the termination of employment, the employee remains obliged to protect the employer's confidential information and trade secrets in accordance with their contractual confidentiality obligations.

Indian courts recognise an employee's contractual obligation to protect an employer's confidential information post-employment. However, the scope of this duty may be narrower than that applicable to confidentiality obligations during employment.

The Delhi High Court in *American Express Bank Ltd. v Ms. Priya Puri (2006 SCC OnLine Del 638)* held that while former employees must respect trade secrets, they are free to use any skills and knowledge acquired during the course of employment.

The Bombay High Court in *Bombay Dyeing and Manufacturing Co. Lt. v Mehar Karan Singh (2010 (112) BomLR 375)* held that an employer cannot prevent the use of an employee's knowledge, skill, and experience even if acquired during the course of employment. Any information carried in the employee's memory may be used post-termination of their employment. However, they cannot directly copy and use any confidential information, such as customer lists, to harm their former employer.

Other Related Duties

Criminal Laws

Indian criminal laws impose penalties (such as fines or imprisonment) on employees for the unauthorised disclosure of confidential information during and after termination of employment. Imprisonment terms for such offences may range from six months to seven years.

The following offences under the *Bharatiya Nyaya Sanhita, 2023*(Criminal Code) (which replaced the Indian Penal Code 1860 and came into effect on 1st July 2024) are relevant in this context:

- Theft by a clerk or a servant in possession of their employer's property (section 306).
- Dishonest misappropriation of property (section 314).
- Criminal breach of trust (section 316).
- Cheating (section 318).

The Information Technology Act, 2000 (IT Act) covers confidential information in digital form and imposes penalties for computer related offences including dishonestly receiving stolen computer resources or communication devices, hacking and unauthorised access to digital data, tampering with computer source documents and cyberterrorism. The IT Act applies if the employee discloses the employer's confidential information during and after termination of employment. Penalties may include imprisonment of up to three years and fines of up to INR500,000.

Protection of Trade Secrets
There is no specific law relating to the protection of trade secrets in India. Employers can seek to protect trade secrets beyond the term of employment by incorporating robust confidentiality clauses to that effect in their employment contracts, non-disclosure agreements, and any company policies.

Confidentiality Clauses in Employment Contracts

Standard clause, Confidentiality Clause for Employment Contract (UK Style) (Jurisdiction Neutral) can be included in employment contracts in India and should be valid and enforceable.

Written Confidentiality Clause

For a contract to be valid and legally binding, it must meet the criteria under the Indian Contract Act, 1872 and must possess the following essential elements:

- A lawful offer and acceptance.
- The mutual consent of the parties.
- A lawful object.
- The parties must have the legal capacity to enter into and execute the contract.
- There must be valid and lawful consideration, such as payment or service.

Additionally, the contractual obligations should be reasonable in scope, duration, and applicability. Contractual provisions which are overly restrictive or burdensome on the employee may be viewed as violating public policy and therefore unenforceable.

The Indian Contract Act, 1872 recognises both written and oral contracts. However, to ensure that there is no ambiguity in the confidentiality obligations and the nature of confidential information that is being protected contractually, a clause such as *Standard clause, Confidentiality Clause for Employment Contract (UK Style) (Jurisdiction Neutral)* should be included in a written contract.

It is standard practice for employers to include a confidentiality clause in individual employment contracts. While the employment contract of employees involved in research, development, coding, and so on will contain detailed confidentiality obligations, the employment contract of a manual labourer or service industry worker may be simpler, with basic confidentiality provisions.

Language

A valid and enforceable contract should be in a language that the employee can read and understand.

Execution Formalities

The contract may be executed using various methods, including:

- **Wet signature.** A handwritten signature.
- **Digital signature certificates.** A secure digital signature issued by a certifying authority.
- **Electronic signatures.** An electronic indication of consent or an electronic authentication process.

To be considered valid evidence in a court of law, the employment must be properly stamped with the required amount of stamp duty (as per applicable stamp duty laws) prior to execution. However, failing to stamp the contract does not necessarily make it invalid.

Definitions

Confidential Information

There is no specific definition of "confidential information" in Indian law. Confidential information is commonly defined in the employment contract and any confidentiality agreement. The definition typically includes all information accessed by, or communicated to, the employee during employment, including:

- All marketing, technical, engineering, operational, economic, security, financial or legal know-how, processes, designs, charts, consents, ideas, systems, project plans and so on.
- An employer's intellectual property and inventions.
- Customer and vendor information.
- The identity and job descriptions of the employer's personnel.
- The employer's organisational structure and business plans.
- An employee's compensation or benefit details.

The confidentiality agreement may specify that confidential information can take any form:

- Graphic.
- Written or verbal.
- Electronic or machine-readable form stored on any media.

Regardless of whether the information is expressly marked or stated to be confidential, it can still be treated as such when defining confidential information.

Additionally, the confidentiality obligation does not extend to information that is already available in the public domain (unless the employee's breach of confidentiality obligations is the reason it became public) (see *Information Existing in the Public Domain*).

There is no statutory limitation on information that can be protected by employers under contractually agreed terms with its employees. Indian courts have permitted the protection of:

- Trade secrets (*Hi Tech Systems and Services Ltd. v Suprabhat Ray, AIR 2015 Cal 261*).
- Industrial drawings (*Escorts Const. Equipment Ltd v Action Const. Equipment Pvt. Ltd., AIR 1999 Delhi 73*).
- List of clients and customers (*Burlington Home Shopping Pvt. Ltd. v Rajnish Chibber, 61 (1995) DLT 6*).
- Proprietary drafts included in the employer's database (*Diljeet Titus v. Mr. Alfred A. Adebare and Others, 2006 (32) PTC 609 (Del)*).

To ensure that the confidential information sought to be protected belongs to the employer, employers must ensure employees assign the intellectual property and inventions created and developed in course of employment to them. It is therefore common to include intellectual property assignment provisions in the employment contract.

Additonally, the employer should also specify that the employees must not:

- Improperly use or disclose any confidential information belonging to a third party.
- Bring any confidential or proprietary information or property belonging to a third party on to the employer premises, without obtaining prior written consent from the third party or without the prior knowledge and consent of the employer.

Protected Corporate Entities

The confidential information of the employer, employer's affiliates, group companies, subsidiaries, and holding companies can be protected under the contract of employment.

In India, the concept of a "group of companies" is recognised in certain limited instances under arbitration and banking laws. The definition provided under *Standard clause, Confidentiality Clause for Employment Contract (UK Style) (Jurisdiction Neutral)* can be used to define a "group of companies" namely:

> "**Group Company:** the Company, its Subsidiaries or Holding Companies from time to time and any Subsidiary of any Holding Company from time to time."

The terms "subsidiary company" and "holding company" are defined under the *Companies Act, 2013* (Companies Act). To provide clarity, the *Standard clause, Confidentiality Clause for Employment Contract (UK Style) (Jurisdiction Neutral)*, may be modified to specify that the definitions of these terms will be defined under the Companies Act. The definition states:

> "**Subsidiary and Holding Company:** in relation to a company mean "subsidiary" and "holding company" as defined under the applicable legislation."

Information Existing in the Public Domain

While it is not a mandatory legal requirement, it is common practice to exclude information already available in the public domain from confidentiality restrictions in employment or confidentiality agreements.

In *Central Public Information Officer, Supreme Court of India v Subhash Chandra Agarwal (2020) 5 SCC 481*, the Supreme Court held that information which is public knowledge and in the public domain cannot be regarded as confidential.

Best Endeavours to Protect Confidential Information

The concept of reasonable efforts or best endeavours is recognised by Indian courts. Accordingly, *Standard clause, Confidentiality clause for Employment Contract (UK Style) (Jurisdiction Neutral): clause 1.3* can be used in confidentiality clauses.

Return of Confidential Information

The language provided in the *Standard clause, Confidentiality Clause for Employment Contract (UK Style) (Jurisdiction Neutral): clause 1.4(b)* can be included in a confidentiality clause in employment contracts in India.

This sub-clause states:

> "All Confidential Information and Copies shall be the property of the Company and on termination of the Appointment, or at [our OR the Board's] request, at any time during the Appointment, you shall:
>
> (b) irretrievably delete any Confidential Information (including any Copies) stored on any magnetic or optical disk or memory, including personal computer networks, personal e-mail accounts or personal accounts on websites, and all matter derived from such sources which is in your possession or under your control outside the Company's premises."

It is common practice for employers to request confirmation from employees that they have complied with the employer's confidentiality obligations and returned all property belonging to the employer before being released from their duties. Employers often execute a release or separation agreement with exiting employees to obtain such confirmation.

Relieving Letters

In India, employers may be legally required to issue a service certificate to exiting employees, however there is no legal requirement for employers to provide a relieving letter to employees.

A service certificate is legally prescribed under the model standing orders in some states such as Haryana (Gurgaon). It is also mandatory for contractors to provide this for contract workers.

The practice of providing a relieving letter to employees who have resigned from the company is more of an industry norm as it helps prospective employers to verify that the candidate has been effectively released from their previous employment duties. To that extent, the provision of a relieving letter is subject to the employer's discretion and is typically issued after the employee has completed all necessary exit formalities, including their obligations to return the employer's confidential information.

Remedies

During Employment

If an employee breaches any confidentiality obligations during the course of their employment, the employer may initiate disciplinary action against the employee.

If the employee holds a managerial position, and is not classified as a "workman" under Industrial Disputes Act, 1947, or is not protected from termination under a state-specific Shops and Establishments Act (such as those applicable to managerial employees in Maharashtra (Mumbai)), employers may have the flexibility to take action against the employee for breaching confidentiality obligations, but only in accordance with the terms of the employment contract.

Post-Employment

The employer may issue a cease-and-desist or legal notice to employees who have breached their post-employment obligations, to prevent further use of the confidential information. If the employer has initial evidence regarding the employee's breach of confidentiality obligations, the employer can seek an interim injunction against the employee and sue for damages. In this instance, the employer must provide the initial evidence of the breach or infringement, which has caused irreparable damage to the employer's business.

Practical Steps

Employers may proactively protect their confidential information and trade secrets from unauthorised use or disclosure by employees. Such steps may include:

- **The implementation of robust contracts and policies.** Employers should include clear confidentiality clauses in employment contracts, policies or standing orders highlighting the types of information considered confidential and the consequences of unauthorised disclosure. A comprehensive non-disclosure agreement may also be executed with employees, outlining specific expectations for handling sensitive information including after employment ends.
- **Having robust information security and privacy policies.** Employers should ensure that they have robust policies that lay down how confidential information (and any sensitive personal data and information) may be used by employees. These policies should also include a restriction on sharing an employer's confidential information outside the employer's systems without prior written approval.
- **Using appropriate technology for monitoring usage of confidential information.** Employers should invest in technology and software that helps monitor the leaking of confidential information or restrict the use of websites and software that may cause security breaches and compromises the confidentiality of the employer's proprietary data and information. To establish a record of sharing confidential information with employees, employers can maintain logbooks or similar documentation, to serve as evidence of the information shared, with whom, and when, in case of future disputes or allegations of breach of confidentiality.
- **Conduct training on confidentiality.** To ensure that employees are aware of and understand their responsibilities regarding information security and confidentiality, employers should provide regular training programmes, helping to prevent breaches and protect sensitive information.

Whistleblowing

Whistleblowing is recognised in India.

Currently, the laws in India that govern whistleblowing are limited in scope to public servants and listed companies, namely:

- Public servants and public sector undertakings which are covered under the Whistle Blowers Protection Act, 2014 (Whistle Blowers Protection Act) (although this law has not yet been implemented).

  The provisions of the Whistle Blowers Protection Act will come into force on such date as the Indian Central Government may appoint, by notification in the official gazette.

- Listed companies regulated under the Companies Act and Securities Exchange Board of India (SEBI) guidelines.

Whistleblower Regulation for Government Sector

The Whistle Blowers Protection Act prohibits the disclosure of any information in connection with any inquiry into a whistleblowing complaint that may affect the following:

- Interest of sovereignty and integrity of India.
- Security of the state.
- Friendly relations with a foreign state.
- Public order, decency or morality or in relation to contempt of court.
- Defamation of incitement to an offence involving the disclosure of proceedings of union or state parliament.

The Whistle Blowers Protection Act (once effective) requires:

- The identity of, and information shared by, a whistleblower to be kept confidential.
- The whistleblower and individuals assisting in any complaint to be protected against victimisation.

Under the Public Interest Disclosure and Protection of Informers Resolution, 2004 (passed by the Indian Government), the Central Vigilance Commission, as the designated agency, is responsible for receiving and handling written complaints or disclosures related to allegations of corruption or misuse of office by:

- Employees of the Central Government.
- Those working in:
  - Corporations established by or under any Central Act.
  - Government companies or local authorities that are owned or controlled by the Central Government.

Whistleblower Regulation for Non-Government Sector

The following Indian companies are required to establish a vigil mechanism:

- Companies which accept deposits from the public.
- Companies that borrow money from banks and public financial institutions in excess of INR50 crore (approximately USD6 million).

(Section 177(9) of the Companies Act.)

For companies that are not subject to this requirement, the Board of Directors can nominate a director to play the role of audit committee for the purpose of the vigil mechanism, to whom other directors and employees can report their concerns.

A vigil mechanism allows employees and directors to report genuine concerns against such companies, ensuring a safe and confidential reporting process.

Indian companies listed on a recognised stock exchange, as regulated by SEBI, are required to have a whistleblower policy in place. This policy must allow employees to report:

- Unethical behaviour.
- Actual or suspected fraud.
- A violation of the company's code of conduct or ethics policy.

Additionally, listed companies and asset management companies must have a whistleblowing policy that covers the reporting of leaks of unpublished price sensitive information (UPSI) as per the SEBI (Prohibition of Insider Trading) Regulations, 2015. These regulations also provide incentives for whistleblowers to encourage the reporting of potential wrongdoing.

The Companies Act and SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 and SEBI (Prohibition of Insider Trading) Regulations, 2015 require companies to provide adequate safeguards against victimisation of directors, employees, and any other individuals who report concerns. There is no statutory guidance in relation to what amounts to victimisation. Typically, it is understood to mean no retaliation against a complainant. There is currently also no specific legal guidance or prescribed requirements outlining the necessary safeguards to protect whistleblowers. Therefore, this will be guided by the employer's policies.

Also, there are requirements under Companies (Auditor's Report) Order, 2020 for all companies to disclose details about certain whistleblower complaints to their statutory auditors.

Confidentiality Clause: Validity in Relation to Whistleblowing

Generally, confidentiality clauses are not automatically considered void if they restrict whistleblowing. However, companies who are required to have a vigil mechanism in place must also have adequate safeguards to protect whistleblowers against being victimised. Accordingly, if an employee breaches a confidentiality obligation to report wrongdoing or unethical behaviour, any action taken by the company in response to the breach should be handled sensitively.

There is no legal requirement to have a "carve out" in the confidentiality clause specifically for whistleblowers or to refer to the legislation governing whistleblowing in *Standard clause, Confidentiality Clause for Employment Contract (UK Style) (Jurisdiction Neutral): clause 1.5*. The current language may be retained in India. This clause states:

> "Nothing in this Clause 1 shall prevent you from [whistleblowing OR equivalent wording] within the meaning of the applicable legislation."

In practice, since not all private employers in India have an obligation to have a whistleblower policy in place, a severability provision should be incorporated into the employment contract or confidentiality agreement, instead of having a specific carve out for whistleblowers as suggested in *Standard clause, Confidentiality Clause for Employment Contract (UK Style) (Jurisdiction Neutral): clause 1.5*.

END OF DOCUMENT