

Employee Confidentiality, Non-Disclosure, Intellectual Property and Business Protection Policy

tCognition Consultancy Pvt. Ltd.

Policy owner: Human Resources Department

Approved by: tCognition Management Team

Applies to: All current and future employees of tCognition Consultancy Pvt. Ltd. and related entities in India that formally adopt this Policy

Effective date: Upon management approval and official publication

Version: 1.0

1. Purpose

This Policy establishes standards for protecting confidential information, intellectual property, business records, client and partner information, and other proprietary assets entrusted to tCognition Consultancy Pvt. Ltd. (the “Company”). It supplements applicable employment obligations and previously executed agreements; it does not replace or automatically amend them.

2. Scope

This Policy applies automatically, as an internal employment policy, to all current and future employees of tCognition Consultancy Pvt. Ltd. and to employees of its subsidiaries, affiliates, group companies and other related entities in India that formally adopt this Policy through authorized management. Coverage includes employees working at offices, remotely, at client locations, or serving notice periods, irrespective of designation or department. For covered employees, the Policy takes effect upon official publication and communication by their employing entity; no separate signature or NDA is required solely to acknowledge these internal standards. Applicability and enforcement remain subject to applicable law, employment terms, and any legally required consultation or procedures. Publication does not by itself create new contractual post-employment restrictions or bind employees of entities that have not adopted the Policy. Employees who separated before the effective date are not covered by new provisions, although existing valid contractual and legal obligations may continue.

3. Confidential Information

Confidential Information means non-public information obtained, accessed, developed, or entrusted to an employee in connection with Company work, including customer and supplier identities and records; contracts, proposals, pricing and financial data; business plans and strategies; source code, system designs, credentials, technical specifications, research and project materials; personnel and recruitment information; personal data; trade secrets; and confidential third-party information. It may be written, electronic, verbal, or otherwise recorded. Information that becomes public without breach, is lawfully received without restriction, or is independently developed without use of protected information is not covered merely because it concerns a similar subject.

4. Employee Responsibilities

Employees must use Confidential Information only for authorized business purposes; limit access to those with a legitimate need; follow approved security practices; and obtain authorization before copying, transmitting, publishing, or disclosing protected material. Employees must not use such information for personal gain or for an unauthorized third party. Employees must promptly report suspected loss, unauthorized access, or disclosure to their manager and the designated information-security or HR contact.

5. Client and Business Relationship Protection

During employment, employees must not improperly divert Company business opportunities, use Company resources or Confidential Information to solicit competing business, or induce clients, suppliers or colleagues to breach their obligations to the Company. Following employment, employees remain bound by valid confidentiality, intellectual-property and other legally enforceable obligations. This Policy does not prohibit lawful post-employment work for a competitor, client or other organization, nor does it create a new post-employment non-compete or non-solicitation covenant.

6. Intellectual Property and Work Product

Employees must comply with applicable law and any existing valid written intellectual-property assignments. Work product created in the course of assigned duties, including software, documentation, designs, reports and related materials, must be documented, stored and delivered through Company-approved systems. Nothing in this Policy independently transfers rights beyond those arising under applicable law or valid agreements.

7. Data Protection and Information Security

Employees must follow Company-approved access controls, password and device practices, data-retention requirements, and instructions for handling personal data. Confidential or personal data must not be uploaded to unapproved cloud services, personal email accounts, external storage, or AI tools. Legally protected disclosures, regulatory reporting, and other rights under applicable law are not restricted by this Policy.

8. Return and Deletion of Company Materials

On request or upon separation, employees must return Company devices, documents, records, access tokens and other property, and cooperate in the transfer of work materials and authorized deletion of Company information from personal devices or accounts, subject to law and legitimate preservation requirements. Employees must not retain unauthorized copies.

9. Continuing Obligations

Confidentiality obligations continue after employment for as long as the information remains protected under an applicable agreement or law. Existing signed NDAs remain effective according to their valid terms. Nothing here extends the duration of an existing contractual restriction or creates a blanket indefinite restriction on publicly available information.

10. Compliance and Consequences

The Company may investigate suspected violations fairly and take proportionate action, including access restrictions, disciplinary measures and lawful civil or other remedies, subject to applicable law, employment terms and any applicable standing orders. No provision guarantees an injunction or other court remedy; such relief is determined by the competent court.

11. Policy Administration and Updates

Human Resources administers this Policy in coordination with authorized management and information-security personnel. Each related legal entity must formally adopt the Policy before applying it to its employees. The relevant employing entity may revise its policy prospectively and communicate updates through official channels, subject to applicable law and employment terms. Employees are expected to review and follow lawful policy requirements; lack of a separate acknowledgement does not by itself establish consent to new contractual terms.

12. Governing Law

This Policy is interpreted under the applicable laws of India for employees of adopting Indian entities. Disputes shall be brought before courts or authorities having jurisdiction under applicable law.

Publication and Contact

This Policy is published for employee reference on the Company website and through official HR channels. Employees should direct policy questions, suspected disclosures, and requests for clarification to the Human Resources Department through approved Company communication channels.