TAKSHAY LABS PRIVATE LIMITED

Research, AI and Digital Security Integrity Policy

Issued by
Takshay Labs Private Limited

Registered Office:
No 3, 6th B Main Road, N S Palya
BTM Layout, Bengaluru Urban
Karnataka 560076, India

Effective Date: 21 January 2026
Policy Version: 1.0

This Policy establishes binding institutional standards governing research integrity, artificial intelligence governance, and digital security for Takshay Labs Private Limited.

Document Control

Field	Details
Document Title	Research, AI and Digital Security Integrity Policy
Issuing Entity	Takshay Labs Private Limited
CIN	U74110KA201PTC086671
Applicable Law	Copyright Act 1957; Information Technology Act 2000; IT (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021; IT (SPDI) Rules 2011; CERT-In Directions 2022; Digital Personal Data Protection Act 2023
Version	1.0
Effective Date	21 January 2026
Last Updated	21 January 2026
Approved By	Mr Satish Shekar, Co-Founder
Document Status	Finalised Version 1.0

Table of Contents

1 Definitions

In this Policy, unless the context otherwise requires, the following terms shall bear the meanings ascribed to them:

"Analytical Framework" means any programme design methodology, institutional coordination model, structural analysis approach, research framework, or other proprietary analytical system developed by the Company or the Founding Team, whether or not reduced to writing and whether or not published on the Website.

"Artificial Intelligence Tools" means any software system, platform, or application that employs machine learning, deep learning, large language models, natural language processing, generative modelling, or any other form of computational artificial intelligence, including but not limited to generative AI systems, AI-assisted research platforms, and automated text or content generation tools.

"AI Training" means the use of any data, text, content, or material for the purpose of training, fine-tuning, pre-training, instruction-tuning, reinforcement learning, or otherwise developing, improving, or adapting any Artificial Intelligence Tool, machine learning model, or automated data processing system.

"Automated Extraction" means any systematic, automated, or programmatic access to, collection of, or extraction of Website Content or data from the Website, including through the use of web crawlers, bots, spiders, scrapers, application programming interfaces, or any other automated mechanism, irrespective of technical method or commercial intent.

"CERT-In" means the Indian Computer Emergency Response Team established under Section 70B of the Information Technology Act 2000, as the national nodal agency for responding to cybersecurity incidents in India.

"Company" means Takshay Labs Private Limited, a company incorporated under the Companies Act 2013 bearing Corporate Identification Number U74110KA201PTC086671, having its registered office at No 3, 6th B Main Road, N S Palya, BTM Layout, Bengaluru Urban, Karnataka 560076, India.

"Content" means all text, articles, analyses, reports, institutional commentary, programme descriptions, research outputs, data compilations, design elements, graphics, audio-visual materials, code, and any other material published or made accessible through the Website, whether or not expressly marked as proprietary.

"Founding Team" means the co-founders and original members of Takshay Labs Private Limited who contributed to the development of the Company's intellectual property, research methodologies, and institutional frameworks in their capacity as employees, officers, or principals of the Company.

"Legitimate Access" means access to the Website and its Content in accordance with the Terms of Use applicable to the Website, solely for personal, non-commercial, informational purposes, and in compliance with all applicable law.

"Material Interest" means any financial, personal, professional, or institutional interest that could reasonably be expected to influence, or to appear to influence, the objectivity, independence, or integrity of any research, editorial, or analytical output of the Company.

"Responsible Disclosure" means the practice of reporting a Security Vulnerability to the Company in a manner that allows the Company a reasonable opportunity to investigate and remediate the vulnerability prior to any public disclosure, in accordance with the procedure set out in Clause 15 of this Policy.

"Security Vulnerability" means any weakness, flaw, misconfiguration, or error in the Website, its underlying infrastructure, software, or associated systems that could be exploited by an unauthorised party to gain access to, disrupt, or compromise the Website, its data, or its associated systems.

"Website" means the official institutional website of the Company accessible at www.takshay.in, including any subdomains, microsites, successor digital properties, or associated web-based platforms operated by the Company.

"Working Days" means days on which commercial banks are open for business in Bengaluru, Karnataka, India, excluding Saturdays, Sundays, and public holidays declared under applicable law.

2 Scope and Applicability

This Policy applies to:

- All members of the Founding Team and all employees, consultants, contractors, and agents of the Company engaged in research, editorial, content creation, technology, or security functions;
- All Content published on or through the Website;
- All Artificial Intelligence Tools utilised by the Company in the course of its internal and external operations;
- All Users who access the Website, to the extent that the provisions of this Policy impose obligations upon or are relevant to such Users.

This Policy applies to the Company's operations within the territory of India and, where applicable, to operations that have legal effect in India under the Information Technology Act 2000 and the Digital Personal Data Protection Act 2023.

This Policy is effective from 21 January 2026 and supersedes any prior internal research integrity, AI governance, or security disclosure guidelines issued by the Company.

3 Relationship with Other Policies in the Suite

This Policy forms part of the Company's institutional governance policy suite, which comprises the following instruments:

- Privacy and Data Protection Policy;
- Governance, Transparency and Accessibility Policy;
- Website Terms of Use and Legal Disclaimer;
- Copyright and Content Usage Policy.

This Policy is to be read in conjunction with the foregoing instruments. In the event of any conflict between this Policy and any other instrument in the policy suite on a matter falling within the scope of this Policy, the provisions of this Policy shall prevail to the extent of the conflict. In the event of any conflict on a matter of data protection, the provisions of the Privacy and Data Protection Policy shall prevail.

The Company may from time to time issue supplementary guidelines, procedures, or guidance notes that expand upon or implement the provisions of this Policy. Such supplementary instruments shall, upon publication, form part of the governance framework of the Company and shall be read in conjunction with this Policy.

4 Institutional Editorial Standards

The Company hereby affirms its commitment to maintaining the highest standards of institutional integrity, accuracy, and objectivity in all Content published through the Website. All Content published by the Company shall comply with the following editorial standards:

- All factual claims must be supported by credible, verifiable sources;

- All analytical and research outputs must accurately represent the evidence and reasoning on which they are based;
- Content must not be presented in a manner that is misleading, deceptive, or calculated to misrepresent the Company's institutional positions;
- Content must be presented in a manner that is fair, balanced, and consistent with applicable legal and ethical standards.

The Company shall maintain internal editorial procedures to ensure compliance with the standards set out in this Clause. Such procedures shall include pre-publication review, editorial sign-off by an authorised member of the Founding Team, and periodic review of published Content for continued accuracy.

5 Research Integrity Principles

The Company adopts the following research integrity principles as binding institutional standards applicable to all research and analytical outputs published through the Website:

- Honesty: All research and analytical outputs shall be conducted and reported honestly. Data, findings, and conclusions shall not be fabricated, falsified, or misrepresented.
- Rigour: Research and analysis shall be conducted with appropriate methodological rigour, employing sound methods of inquiry and analysis relevant to the subject matter.
- Transparency: The sources, methodologies, and assumptions underlying research outputs shall be disclosed to the extent practicable and appropriate to the nature of the output.
- Independence: Research outputs shall represent the independent assessment of the Founding Team and shall not be distorted to serve external interests.
- Accountability: The Company accepts institutional responsibility for the accuracy and integrity of research outputs published through the Website.

Pursuant to the provisions of the Copyright Act 1957, all original research outputs created by the Founding Team in the course of their engagement with the Company constitute literary works in which copyright vests in the Company as employer pursuant to Section 17 of the Copyright Act.

6 Editorial Independence

The Founding Team exercises editorial independence in the selection of research topics, the formulation of analytical positions, and the publication of Content through the Website. No external party, including clients, funders, partners, or other stakeholders, shall have the authority to direct, control, or unduly influence the editorial decisions of the Company.

The Company hereby affirms that:

- Editorial decisions are made solely by authorised members of the Founding Team;
- No person or entity external to the Company has authority to require the publication, amendment, or removal of any Content on the Website as a condition of any commercial, funding, or partnership arrangement;
- Any institutional arrangement with an external party that could give rise to a perception of editorial compromise shall be disclosed in accordance with Clause 12 of this Policy.

This Clause does not preclude the Company from voluntarily considering the views and feedback of external parties, provided that editorial decisions remain the independent determination of the Founding Team.

7 Fact Verification and Source Integrity

The Company shall implement and maintain a fact verification procedure applicable to all factual claims published in Content through the Website. Such procedure shall include the following:

- Identification and verification of primary or credible secondary sources for factual claims;
- Cross-referencing of factual claims with at least one independent, verifiable source where practicable;
- Review of claims that are contested, sensitive, or relate to third parties for accuracy and fairness prior to publication;
- Retention of source documentation to support factual claims for such period as is consistent with the Company's document retention practices.

The Company shall not knowingly publish Content that contains factually incorrect statements. In the event that a factual error is identified in published Content, the Company shall correct such error in accordance with the procedure set out in Clause 13 of this Policy.

Where Content incorporates data or information derived from third-party sources, appropriate attribution shall be provided in accordance with the citation and attribution requirements set out in the Copyright and Content Usage Policy.

8 Governance of Artificial Intelligence Tools

8.1 Permitted Use of Artificial Intelligence Tools

The Company may utilise Artificial Intelligence Tools to support research, editorial, and operational workflows, including but not limited to research summarisation, drafting assistance, data analysis, and administrative tasks. The use of Artificial Intelligence Tools by the Company is subject to the governance principles set out in this Clause and in Clauses 9 and 10 of this Policy.

8.2 Governance Principles

The Company's use of Artificial Intelligence Tools shall be governed by the following principles:

- Accountability: The Company accepts institutional responsibility for all Content published through the Website, irrespective of whether Artificial Intelligence Tools were used in its preparation.
- Human Primacy: Artificial Intelligence Tools shall be used only to augment and support human research and editorial work. No Artificial Intelligence Tool shall be permitted to exercise autonomous decision-making authority over the content, framing, or publication of any research or analytical output.
- Transparency: The Company shall maintain internal records of the categories of Artificial Intelligence Tools used in the preparation of Content, to the extent reasonably practicable.
- Data Protection: Artificial Intelligence Tools shall not be used to process Personal Data of Users in contravention of the Digital Personal Data Protection Act 2023 or the Company's Privacy and Data Protection Policy.
- Ethical Use: Artificial Intelligence Tools shall not be used to generate misleading, deceptive, or harmful content, to impersonate individuals or institutions, or to simulate official or governmental authority.

8.3 Multiple AI Platforms

The Company may utilise multiple Artificial Intelligence Tools across different operational functions. No single Artificial Intelligence Tool constitutes the exclusive operational system of the Company. The

specific tools deployed by the Company may be updated, replaced, or supplemented over time in accordance with operational requirements, quality standards, and applicable law.

9 Mandatory Human Editorial Oversight

The Company hereby affirms that all Content prepared with the assistance of Artificial Intelligence Tools is subject to mandatory human editorial review and approval prior to publication through the Website. No AI-assisted Content shall be published without the prior review and sign-off of an authorised member of the Founding Team or a designated editorial officer of the Company.

The mandatory human editorial oversight process shall include the following:

- Review of AI-assisted Content for factual accuracy, completeness, and consistency with the Company's research integrity principles set out in Clause 5;
- Verification that AI-assisted Content does not contain fabricated citations, hallucinated data, or other inaccuracies introduced by Artificial Intelligence Tools;
- Assessment of AI-assisted Content for alignment with the Company's editorial standards, institutional positions, and applicable legal requirements;
- Final editorial approval by an authorised human editor prior to publication.

The Company shall maintain internal records of the editorial review and approval process for AI-assisted Content for a minimum period of two years from the date of publication, or such longer period as may be required by applicable law.

10 Restrictions on AI Training and Automated Data Extraction

The Company hereby affirms that:

- All Content published on the Website is the intellectual property of the Company and is protected by copyright pursuant to the Copyright Act 1957;
- No Content may be used for AI Training, whether for commercial or non-commercial purposes, without the prior express written consent of the Company;
- Automated Extraction of Content from the Website is prohibited without the prior express written consent of the Company.

The following specific prohibitions apply:

- The use of any Content for the training, fine-tuning, pre-training, or instruction-tuning of any Artificial Intelligence Tool, large language model, or machine learning system is expressly prohibited;
- The ingestion, indexing, or processing of Content by any automated system for the purpose of building a dataset, corpus, training set, or evaluation benchmark is prohibited;
- Systematic Automated Extraction of Content through web crawlers, bots, spiders, or other programmatic means is prohibited, subject to any express permission granted by any robots.txt instruction published by the Company;
- The circumvention of any technological protection measure implemented by the Company to prevent Automated Extraction is prohibited pursuant to Section 65A of the Copyright Act 1957.

Any entity operating a web crawler, AI training pipeline, or automated data collection system must obtain express written permission from the Company at info@takshay.com prior to accessing, processing, or utilising Content for any such purpose.

11 Protection of Analytical Frameworks and Research Content

The Company's Analytical Frameworks constitute original works of authorship and proprietary intellectual property of the Company. Such Analytical Frameworks are protected as literary and artistic works under Section 13 of the Copyright Act 1957, as compilations and original expressions of ideas, methods, and processes developed by the Founding Team.

The following protections apply to Analytical Frameworks:

- No person may reproduce, adapt, translate, or create derivative works based on any Analytical Framework without the prior express written consent of the Company;
- No person may use any Analytical Framework for commercial purposes, including in the provision of consulting, advisory, research, or training services, without the prior express written consent of the Company;
- No person may present any Analytical Framework as their own work or misrepresent its provenance or authorship.

The protection afforded to Analytical Frameworks under this Clause is without prejudice to any protection available under the law of trade secrets, confidential information, or any other applicable legal doctrine. The Company reserves the right to pursue all available legal remedies against any person who misappropriates or infringes its Analytical Frameworks.

12 Conflict of Interest Disclosure

The Company is committed to transparency in the disclosure of any actual or perceived conflicts of interest that may affect the objectivity or independence of its research and analytical outputs.

The following disclosure obligations apply:

- Any member of the Founding Team who has a Material Interest in any organisation, project, or matter that is the subject of any Content published through the Website must disclose such Material Interest to the Company prior to the preparation or publication of such Content;
- Where a disclosed Material Interest is assessed as giving rise to an actual or perceived conflict of interest, the relevant member of the Founding Team shall either recuse themselves from involvement in the preparation of the relevant Content, or the Company shall disclose the conflict of interest in the relevant Content at the time of publication;
- Institutional funding arrangements, partnership agreements, or other material financial relationships between the Company and any external party that could affect the Company's editorial independence shall be disclosed on the Website to the extent required by applicable standards of research integrity.

Conflict of interest disclosures shall be maintained in the Company's internal records and shall be reviewed as part of the editorial sign-off process for each piece of Content.

13 Corrections, Editorial Updates and User Correction Requests

The Company is committed to maintaining the accuracy of Content published through the Website. Where a factual error or material inaccuracy is identified in published Content, the Company shall implement the following correction procedure:

- Minor factual errors, typographical errors, or formatting issues may be corrected without the publication of a formal correction notice, provided that the correction does not alter the substantive meaning or conclusions of the Content;

- Significant factual errors or material inaccuracies shall be corrected through the publication of a formal correction notice, clearly identifying the nature of the error and the correction made;
- Where a correction materially alters the conclusions or findings of a research or analytical output, the Company shall publish a revised version of the Content clearly marked as a correction, with the nature of the revision explained.

Users who identify a factual inaccuracy in published Content may submit a correction request to the Company by email at info@takshay.com, providing the following information:

- The URL of the Content containing the alleged inaccuracy;
- A clear description of the alleged inaccuracy and the basis for the correction request;
- Supporting evidence or sources for the proposed correction, where available.

The Company shall acknowledge receipt of correction requests within five (5) Working Days and shall assess all requests in good faith. The Company shall notify the User of its determination within fifteen (15) Working Days of receipt of the request, or such longer period as is reasonably required given the complexity of the matter.

14 Responsible Security Disclosure

The Company is committed to maintaining the security and integrity of the Website and its underlying infrastructure. The Company recognises the importance of responsible disclosure of Security Vulnerabilities and invites good-faith security researchers and users to report Security Vulnerabilities in accordance with the procedure set out in Clause 15 of this Policy.

The Company hereby affirms the following responsible disclosure principles:

- The Company will investigate all reports of Security Vulnerabilities submitted in accordance with Clause 15 in good faith and within a reasonable timeframe;
- The Company will not pursue civil or criminal proceedings against any person who reports a Security Vulnerability in good faith and in compliance with the responsible disclosure procedure, provided that such person has not accessed or compromised any data, systems, or services beyond what is strictly necessary to demonstrate the vulnerability;
- The Company will acknowledge receipt of all responsible disclosure reports and will keep the reporting party reasonably informed of the progress of its investigation;
- The Company may, at its sole discretion, publicly acknowledge the contribution of researchers who report Security Vulnerabilities in good faith, unless the reporting party requests anonymity.

The responsible disclosure principles set out in this Clause do not extend to any person who exploits a Security Vulnerability for malicious, criminal, or commercial purposes, or who discloses a Security Vulnerability publicly before the Company has had a reasonable opportunity to remediate it.

15 Vulnerability Reporting Procedure

Any person who identifies a Security Vulnerability in the Website or its infrastructure must report such vulnerability to the Company by submitting a written report by email to: info@takshay.com

The vulnerability report must include the following information:

- A clear description of the Security Vulnerability, including the affected component, system, or feature of the Website;
- The steps required to reproduce the vulnerability, including any technical details necessary for the Company to verify and assess the report;

- An assessment of the potential impact of the vulnerability, where the reporting party is able to provide such an assessment;
- The name and contact details of the reporting party, or a request for anonymity where the reporting party does not wish to be identified.

The Company shall acknowledge receipt of vulnerability reports within five (5) Working Days of receipt. The Company shall assess all vulnerability reports in good faith and shall implement appropriate remediation measures within a reasonable timeframe, having regard to the severity and complexity of the reported vulnerability.

The reporting party shall not disclose the Security Vulnerability publicly or to any third party before the Company has confirmed that the vulnerability has been remediated, or before a mutually agreed disclosure timeline has elapsed. The Company shall use reasonable efforts to remediate critical Security Vulnerabilities within ninety (90) calendar days of confirmation of the vulnerability.

16 Website Security Practices

The Company implements and maintains the following technical and organisational measures to protect the Website and its infrastructure against unauthorised access, disruption, and security incidents:

- Deployment of secure cloud hosting infrastructure on Amazon Web Services, subject to AWS's security certifications and contractual data protection obligations;
- Encryption of data in transit using Transport Layer Security (TLS) protocols to protect communications between the Website and its users;
- Role-based access controls restricting administrative access to the Website's content management system and backend infrastructure to authorised personnel;
- Regular application of security patches and updates to the Website's content management platform and associated software components;
- Deployment of web application firewall and other network security controls as appropriate to the threat environment;
- Periodic security assessments and vulnerability scans of the Website's infrastructure and applications.

The Company maintains its Website security practices in accordance with applicable requirements under the Information Technology Act 2000, the IT (SPDI) Rules 2011, and the CERT-In Directions 2022. The Company shall review and update its security practices periodically to reflect developments in the threat environment and applicable regulatory requirements.

17 Incident Response and Remediation

In the event of a cybersecurity incident affecting the Website or its infrastructure, the Company shall implement the following incident response procedure:

- Detection and Containment: Upon detection of a cybersecurity incident, the Company shall take immediate steps to contain the incident and prevent further compromise of systems, data, or services;
- Assessment: The Company shall assess the nature, scope, and impact of the incident, including whether any Personal Data has been compromised;
- Notification: Where the incident involves a breach of Personal Data, the Company shall comply with its notification obligations under the Digital Personal Data Protection Act 2023 and the Company's Privacy and Data Protection Policy. Where the incident constitutes a reportable cybersecurity incident under the CERT-In Directions 2022, the Company shall report the incident to CERT-In within the timeframe prescribed under the said Directions;

- Remediation: The Company shall implement appropriate technical and organisational measures to remediate the incident and restore the security and integrity of the Website and its infrastructure;
- Post-Incident Review: Following remediation of the incident, the Company shall conduct a post-incident review to identify the root cause of the incident, assess the effectiveness of the incident response, and implement measures to prevent recurrence.

The Company shall maintain records of all cybersecurity incidents, including the nature of the incident, the measures taken in response, and the outcome of the incident response, for such period as is required by applicable law.

17.1 CERT-In Reporting Obligations

Pursuant to the CERT-In Directions 2022 issued under Section 70B of the Information Technology Act 2000, the Company shall report cybersecurity incidents of the categories specified in the CERT-In Directions to CERT-In within six hours of becoming aware of the incident, or within such other timeframe as may be prescribed by CERT-In from time to time. The Company shall comply with all directions and advisories issued by CERT-In in connection with any cybersecurity incident.

17.2 Legal Enforcement Against Malicious Activity

The Company hereby affirms that it will pursue all available legal remedies against any person or entity that engages in malicious cybersecurity activity against the Website or its infrastructure, including but not limited to:

- Unauthorised access to the Website or its underlying systems, which constitutes an offence under Section 43 and Section 66 of the Information Technology Act 2000;
- Denial of service attacks, data theft, data corruption, malware deployment, or other forms of malicious cyber activity, which may constitute offences under the Information Technology Act 2000 and other applicable law;
- Any activity intended to compromise the integrity, availability, or confidentiality of the Website or its data.

18 Grievance Officer

Pursuant to applicable law, including the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, the Company has designated a Grievance Officer to receive and address complaints, notices, and queries relating to this Policy. The details of the Grievance Officer are as follows:

- Name: Mr Satish Shekar
- Designation: Co-Founder, Takshay Labs Private Limited
- Email: ss@takshay.com
- Address: No 3, 6th B Main Road, N S Palya, BTM Layout, Bengaluru Urban, Karnataka 560076, India
- Business Hours: Monday to Friday, 10:00 a.m. to 6:00 p.m. IST, excluding public holidays

Any User or other person who has a complaint, query, or notice relating to this Policy, including any complaint relating to research integrity, AI governance, or cybersecurity practices, may submit a written communication to the Grievance Officer at the contact details specified above. The Grievance Officer shall acknowledge receipt of the complaint within five (5) Working Days of receipt and shall endeavour to resolve the matter expeditiously and in accordance with applicable law.

19 Policy Governance and Administration

The authority to approve, amend, or revoke this Policy is vested exclusively in the governance leadership of the Company, being the Management of Takshay Labs Private Limited or such person or committee as may be formally designated for this purpose.

This Policy shall be subject to review upon the occurrence of any of the following:

- Any material change to applicable legal or regulatory requirements, including amendments to the Information Technology Act 2000, the Digital Personal Data Protection Act 2023, or any rules, regulations, or directions issued thereunder, including directions issued by CERT-In;
- Any material development in the Company's use of Artificial Intelligence Tools or in applicable AI governance standards;
- Any material cybersecurity incident affecting the Website or its infrastructure;
- Any other development that materially affects the subject matter of this Policy.

In addition to event-triggered reviews, the Company shall conduct a periodic review of this Policy on at least an annual basis to confirm its continued accuracy, adequacy, and relevance.

20 Policy Amendments

The Company reserves the right to amend, modify, update, or replace any provision of this Policy at any time, at its sole discretion and subject to the approval of the Company's governance authority. Amendments shall become effective upon publication of the revised Policy on the Website. The version control information in the Document Control table shall be updated to reflect the effective date and version number of each revised version of this Policy.

The Company shall use reasonable efforts to bring material amendments to the attention of persons to whom this Policy applies by means of a prominent notice on the Website. The absence of individual notification shall not affect the validity or enforceability of any amendment.

21 Transition and Savings Clause

This Policy supersedes all prior internal research integrity guidelines, AI use policies, and security disclosure procedures issued by the Company prior to the Effective Date of this Policy.

Notwithstanding anything contained herein, any rights, remedies, obligations, or liabilities that accrued prior to the Effective Date of this Policy under any prior internal policy or procedure of the Company shall not be extinguished or affected by the coming into force of this Policy. Such rights, remedies, obligations, and liabilities shall continue to be governed by the provisions of the applicable prior policy or procedure.

22 Governing Law and Jurisdiction

This Policy shall be governed by, construed, and enforced in accordance with the laws of the Republic of India, including the Copyright Act 1957, the Information Technology Act 2000, the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, the IT (SPDI) Rules 2011, the CERT-In Directions 2022, and the Digital Personal Data Protection Act 2023.

Any dispute, controversy, or claim arising out of or in connection with this Policy, including any question regarding its validity, interpretation, breach, or enforcement, shall be subject to the exclusive jurisdiction of the courts of competent jurisdiction situate in Bengaluru, Karnataka, India.

Nothing in this Clause shall limit the right of the Company to seek urgent injunctive relief or other interim remedies from any court of competent jurisdiction, whether within or outside India, where the Company determines that such relief is necessary to protect its rights on an urgent basis.

End of Document