

REESECURE

ADDITIONAL TERMS OF SERVICE

Intellectual Property | Trade Secrets | Platform Integrity
Acceptable Use | Non-Circumvention

Reesecure Group

Reesecure Pte. Ltd. | Reesecure IFSC Private Limited (IFSCA, GIFT City)

Effective Date: June 1, 2025 | Version 5.0

MANDATORY SEPARATE ACCEPTANCE — LEGALLY BINDING

These Additional Terms require separate acceptance via a distinct checkbox in addition to the Reesecure Terms of Service. By clicking "I Agree to the Additional Terms of Service", you agree to be bound by these Additional Terms. Without acceptance, access to the Platform is prohibited.

PATENT PORTFOLIO NOTICE

The Reesecure Platform incorporates inventions protected by the Reesecure Patent Portfolio, comprising all issued patents, pending applications, continuations, divisionals, continuations-in-part, and foreign counterparts, whether now existing or filed in the future, owned, licensed, controlled, prosecuted, maintained, or otherwise held for the benefit of Reesecure Group. Certain Platform functionality is protected by issued patents and pending patent applications in India and other jurisdictions. Unauthorised use or replication is prohibited.

1. DEFINITIONS

Capitalised terms used but not defined herein have the meanings given in the Reesecure Terms of Service. In addition:

"Competitive Intelligence" means any systematic activity designed to evaluate, benchmark, compare, map, or assess the Platform for the purpose of informing development, procurement, validation, or improvement of a Competitive Product

"Competitive Product" means any product, service, software, platform, model, or system that provides climate risk analytics, parametric trigger infrastructure, agricultural risk scoring, catastrophe risk scoring, or similar functionality to the Platform

"Ecosystem Partner" means any insurer, reinsurer, bank, NBFC, DFI, lender, custodian, data provider, or capital provider who was introduced to User by or through Reesecure or the Platform, as documented by email, platform records, meeting minutes, CRM records, written introduction, or other contemporaneous evidence

"Internal Governance Use" means use of Platform outputs solely for (a) internal model risk management and governance review; (b) internal regulatory compliance validation required by applicable law; (c) internal audit obligations; (d) credit committee reviews; (e) board and senior management reporting; or (f) regulatory examination responses — provided such use does not involve training, fine-tuning, benchmarking, or improving any model or competing system

"Model Extraction" means any technique or method designed or used to replicate, reconstruct, infer, or approximate the functionality, parameters, thresholds, calibration values, trigger logic, or algorithmic structure of the Platform

"Patent Portfolio" means as defined in the Reesecure Terms of Service — all issued patents, pending applications, continuations, divisionals, continuations-in-part, and foreign counterparts, whether now existing or filed in the future, owned, licensed, controlled, prosecuted, maintained, or otherwise held for the benefit of Reesecure Group in any jurisdiction

"Platform IP" means the Patent Portfolio; all trade secrets; calibration methodologies; climate risk frameworks; trigger parameterisation systems; actuarial models; evidence architectures; underwriting support methodologies; pricing frameworks; algorithms; APIs; software; source code; model weights; inference configurations; system prompts; orchestration workflows; feature engineering pipelines; retrieval architectures; dashboards; documentation; and all related proprietary technology and know-how

"Reesecure Group" means Reesecure Pte. Ltd. (Singapore), Reesecure IFSC Private Limited (IFSCA, GIFT City, India), and any entity directly or indirectly controlling, controlled by, or under common control with either of them

"Trade Secret" means information constituting a trade secret under applicable law, including all Platform IP that is not in the public domain

2. PATENT PORTFOLIO & PATENT-PENDING TECHNOLOGY

2.1 Patent Portfolio Coverage

The Platform incorporates inventions protected by the Patent Portfolio, covering all issued patents, pending patent applications, continuations, divisionals, continuations-in-part, and foreign counterparts, whether now existing or filed in the future, owned, licensed, controlled, prosecuted, maintained, or otherwise held for the benefit of Reesecure Group, in all applicable jurisdictions including India, Singapore, and other PCT member states. Certain Platform functionality is protected by issued patents and pending patent applications in India and other jurisdictions.

2.2 No Patent Licence

Nothing in this Agreement grants User any licence under the Patent Portfolio, except the limited right to use the Platform as expressly permitted in the applicable Order Form. No implied licence arises through any course of dealing, use, disclosure, access, evaluation, pilot, or payment.

2.3 Reservation of Rights

Except for the limited rights expressly granted under this Agreement, Reesecure and its licensors reserve all right,

title, and interest in and to the Platform, Platform IP, Services, and all related intellectual property rights. No rights are granted by implication, estoppel, exhaustion, or otherwise. All intellectual property rights in the Platform and Services are owned by or licensed to Reesecure Group.

2.4 Patent Challenge Prohibition

User shall not directly or indirectly challenge, contest, oppose, or assist any third party in challenging the validity, ownership, enforceability, scope, or registrability of any patent, patent application, trade mark, or other intellectual property owned or controlled by Reesecure Group, except where such restriction is prohibited by applicable law.

2.5 Patent Marking

Platform interfaces may carry patent markings, pending notices, or references to patent filings. User must not remove, obscure, or alter any such notices.

2.6 Protected Technology Categories

The following technology categories are patent-protected or patent-pending. Unauthorised use or replication is strictly prohibited:

- Deterministic parametric trigger evaluation systems and methodologies
- Climate risk scoring algorithms and district-level risk scoring frameworks
- Cryptographic evidence bundle architectures
- Hierarchical capital allocation and risk transfer architectures
- Crop-system-aware parametric trigger libraries with phenological stage integration
- Tamper-proof audit chain architectures
- ECL-integrated climate risk provisioning frameworks
- Multi-stakeholder syndicated risk layer architectures

3. TRADE SECRETS & KNOW-HOW

3.1 Trade Secret Categories

The following categories are Trade Secrets and proprietary know-how of Reesecure Group. These categories are illustrative and not exhaustive:

- Actuarial models and loss estimation methodologies
- Calibration methodologies and parameter selection frameworks
- Climate risk scoring and district-level risk assessment frameworks
- Trigger parameterisation systems and threshold-setting methodologies
- Evidence bundle architectures and cryptographic validation systems
- Underwriting support methodologies and risk stratification frameworks
- Pricing frameworks and commercial structures with data providers
- Proprietary software systems, APIs, and integration architectures
- Source code, system prompts, model weights, inference configurations, orchestration workflows, and retrieval architectures
- Internal training datasets, validation corpora, and data processing pipelines

3.2 Obligations

User agrees to maintain all Platform IP and Trade Secrets in strict confidence and to implement measures at least as protective as those User uses for its own most sensitive proprietary information.

3.3 Trade Secret Exclusions

Information is not a Trade Secret if it: (a) is or becomes publicly available other than through breach; (b) was already known at the time of disclosure, evidenced by contemporaneous written records; (c) is independently developed without reference to Reesecure's Confidential Information; or (d) is lawfully received from a third party without restriction.

3.4 Open Data Exception

Nothing in this Agreement restricts User from using publicly available data, independently developed methodologies, or independently acquired datasets. Reesecure does not claim any proprietary right over raw climate data, publicly available weather data, or publicly available crop data that the Platform may incorporate alongside its proprietary methodology.

3.5 Duration

Trade secret obligations are perpetual and survive termination for so long as the relevant information qualifies as a trade secret under applicable law.

4. REVERSE ENGINEERING & EXTRACTION PROHIBITIONS

ABSOLUTE PROHIBITION — MATERIAL BREACH

The following acts constitute material breach of these Additional Terms, entitling Reesecure to immediate termination and equitable relief.

4.1 Prohibited Acts

User must not, and must ensure that its Authorised Users, contractors, agents, and Affiliates do not, directly or indirectly:

- ✗ Reverse engineer, disassemble, decompile, or otherwise attempt to derive source code, object code, algorithms, or architecture from the Platform;
- ✗ Perform or commission Model Extraction by any means, including systematic API querying, black-box testing, differential analysis, or oracle attacks;
- ✗ Attempt to reconstruct, infer, or approximate trigger thresholds, calibration parameters, weighting coefficients, risk scores, or other model parameters;
- ✗ Intercept, monitor, or analyse network traffic or API calls to infer Platform architecture;
- ✗ Map API behaviour, endpoint structures, or response schemas for the purpose of replication or circumvention;
- ✗ Extract, harvest, or scrape data, parameters, scores, or outputs through automated means including bots, scrapers, or crawlers;
- ✗ Use any side-channel technique, timing attack, or statistical inference method to derive Trade Secrets;
- ✗ Prompt, instruct, or request any third party (including AI services) to assist in reverse engineering or Model Extraction;
- ✗ Attempt to identify, reconstruct, or replicate any evidence bundle architecture, cryptographic protocol, or audit generation methodology; or
- ✗ Reverse engineer any API authentication mechanism, token generation algorithm, or access control system.

5. AI TRAINING, MODEL VALIDATION & MACHINE LEARNING

CRITICAL PROHIBITION

Use of Platform outputs for AI/ML training, fine-tuning, or competitive evaluation purposes is absolutely prohibited, subject only to the Internal Governance Use carve-out in Section 5.3.

5.1 Prohibited Training Uses

User is strictly prohibited from using Platform outputs, APIs, dashboards, scores, analytics, evidence packages, reports, metadata, or any other content derived from the Platform to:

- ✗ Train, fine-tune, pre-train, or post-train any artificial intelligence, machine learning, large language model, foundation model, neural network, or predictive model;
- ✗ Generate synthetic datasets, proxy datasets, distillation datasets, or benchmark corpora from Platform outputs for any AI training purpose;
- ✗ Use Platform outputs as labels, annotations, ground-truth data, or training signals for any machine learning pipeline;
- ✗ Develop or validate any Competitive Product using Platform outputs or derived datasets; or
- ✗ Export Platform outputs as synthetic training datasets, benchmark datasets, or evaluation corpora for foundation models or competing analytical systems.

5.2 Prohibited Validation Uses

User may not use Platform outputs to validate, calibrate, evaluate, benchmark, test, improve, or certify any predictive model, scoring system, underwriting framework, or competing analytical methodology, except as expressly permitted under Section 5.3.

5.3 Internal Governance Carve-Out

Notwithstanding Sections 5.1 and 5.2, User may use Platform outputs for Internal Governance Use, provided such use does not involve training, fine-tuning, or improving any model or competitive system. User shall maintain written records of Internal Governance Use upon reasonable request.

6. BENCHMARKING & COMPARATIVE ANALYSIS

6.1 Restriction

User may not, without prior written consent:

- ✗ Publish, disclose, or distribute any benchmarking results, performance comparisons, or evaluation reports involving the Platform;
- ✗ Compare the Platform to any Competitive Product in any public-facing communication or research paper;
- ✗ Provide benchmarking data to any third party; or
- ✗ Conduct performance tests with the purpose or effect of informing development of a Competitive Product.

6.2 Regulatory & Procurement Carve-Out

User may disclose information about the Platform to the extent strictly required by applicable law, supervisory direction, internal or external audit obligations, internal procurement review obligations, or statutory filing requirements. User shall disclose only the minimum information required and give Reesecure advance notice where practicable.

6.3 Internal Use

User may conduct internal, non-disclosed performance assessments solely for evaluating its own use of the Platform, subject to confidentiality obligations.

7. COMPETITIVE USE, INTELLIGENCE & DERIVATIVE WORKS

7.1 Competitive Use Prohibition

User may not use the Platform for the purpose of:

- ✗ Developing, designing, validating, improving, or commercialising any Competitive Product;
- ✗ Advising or assisting any third party in developing a Competitive Product;

- X** Building internal capability to replicate the core functionality of the Platform; or
- X** Providing technical assessment or validation support for any competitor.

7.2 Competitive Intelligence Restriction

User shall not use the Platform for Competitive Intelligence with the intent of developing or procuring substantially similar functionality from another provider. This restriction does not apply to User's ordinary internal procurement comparison of competing products conducted without reference to Reesecure Confidential Information.

7.3 Output Warehousing

User may not systematically export, compile, aggregate, or warehouse Platform outputs for the purpose of creating a substitute database, benchmark repository, model training corpus, or competing analytical service. Ordinary internal business use of outputs for credit reporting, risk management, and regulatory submissions is not restricted.

7.4 Derivative Works

User may not create or permit others to create any derivative work or adaptation based on Platform IP. All improvements conceived using Confidential Information of Reesecure vest exclusively in Reesecure.

7.5 White-Labeling

Unauthorised white-labelling or OEM distribution of the Platform is strictly prohibited. Any white-label arrangement requires a separate written agreement.

8. NON-CIRCUMVENTION

8.1 Scope

User agrees not to use information obtained through the Platform or through any relationship with Reesecure to bypass, replicate, disintermediate, or circumvent Reesecure in connection with any Ecosystem Partner — defined as a counterparty introduced to User by or through Reesecure and documented by email, platform records, meeting minutes, CRM records, written introduction, or other contemporaneous evidence.

8.2 Covered Relationships

Non-circumvention applies specifically to: (a) introduced data providers, weather oracle providers, and satellite data providers; (b) introduced reinsurers and capital providers; and (c) any commercial arrangement or distribution channel introduced by Reesecure and documented as above.

8.3 Duration

Non-circumvention obligations survive termination for twenty-four (24) months.

8.4 Exclusions

Non-circumvention obligations do not apply where User can demonstrate through contemporaneous written records: (a) a pre-existing relationship with the Ecosystem Partner independent of Reesecure; (b) that the introduction was not the material cause of the relationship; (c) the Ecosystem Partner is a regulatory body or public institution; or (d) the Ecosystem Partner is an investor with whom Reesecure has no current commercial arrangement.

9. API ACCEPTABLE USE

9.1 Permitted Use

API access is limited to programmatic integration with User's own internal systems for purposes specified in the Order Form.

9.2 Prohibited Uses

User must not:

- X** Exceed API rate limits or attempt to circumvent throttling;
- X** Use automated scripts or bots to query the API beyond normal operational requirements;

- ✗ Share or transfer API keys to any third party;
- ✗ Use the API to scrape or extract bulk data for external storage or competitive use;
- ✗ Probe or fuzz the API to identify vulnerabilities or architecture; or
- ✗ Use API responses to populate any Competitive Product database.

10. FEEDBACK & WORK PRODUCT

10.1 Feedback Licence

User retains ownership of its pre-existing intellectual property, processes, methodologies, and know-how. If User provides any suggestions, comments, enhancement requests, corrections, ideas, or improvements relating to the Platform ("Feedback"), including observations arising from sandbox participation, pilots, evaluations, proofs of concept, or regulatory testing activities, User grants Reesecure a perpetual, irrevocable, worldwide, royalty-free, sub-licensable licence to use, incorporate, reproduce, modify, and exploit such Feedback without restriction, compensation, or attribution. Reesecure shall own any improvements, enhancements, or modifications made to the Platform arising from Feedback.

11. BRAND PROTECTION

11.1 Protected Marks

The following marks are proprietary to Reesecure Group. No right to use any of these marks is granted without prior written consent:

- Reesecure® (word mark and logo)
- TriggerFlow™
- VaultX™
- PolicyBoard™
- Reesecure Network™
- District Climate Risk Score™ / DCRS™

11.2 Restrictions

User must not register any Reesecure mark or confusingly similar mark; use any mark in User's own trade name or product; or use any mark in meta-tags, paid search, or investor presentations in a manner that misrepresents the relationship between User and Reesecure.

12. CONFIDENTIAL INFORMATION

12.1 Heightened Obligations

In addition to the confidentiality obligations in the Terms of Service, User agrees to:

- Restrict access to Platform IP to Authorised Users with a need to know;
- Implement role-based access controls, audit logging, and session management;
- Promptly notify Reesecure of any suspected or actual unauthorised disclosure within twenty-four (24) hours; and
- Cooperate fully with any investigation of unauthorised disclosure.

12.2 Trade Secret Exclusions

The trade secret exclusions in Section 3.3 apply equally to all Confidential Information obligations under this Section 12.

12.3 Regulatory Disclosure

Where disclosure is required by applicable law, regulation, or supervisory direction, User may make such disclosure to the minimum extent required, subject to the conditions in Section 8 of the Terms of Service (Regulatory Carve-Outs).

13. IP COMPLIANCE VERIFICATION

13.1 Documentary Verification

Upon reasonable written notice, Reeseure may request reasonable documentary evidence sufficient to verify User's compliance with these Additional Terms. Such verification shall be limited to relevant records, API usage logs, and written certifications. Reeseure shall not require access to User's internal systems, development repositories, or personnel without User's express written consent.

13.2 Expedited Verification

In the event of suspected material breach of Sections 4, 5, 7, or 8, Reeseure may request expedited documentary evidence with a response period of no less than five (5) business days.

14. REMEDIES & EQUITABLE RELIEF

IRREPARABLE HARM — EQUITABLE RELIEF

User acknowledges that any breach of Sections 4, 5, 7, 8, or 12 will cause irreparable harm to Reeseure for which monetary damages would be an inadequate remedy.

14.1 Available Remedies

In the event of breach, Reeseure may seek any and all remedies available at law or in equity, including:

- Injunctive or other equitable relief where monetary damages would be inadequate;
- Actual damages, including all demonstrable losses, lost profits, and lost business opportunities;
- Recovery of Reeseure's profits attributable to the infringement or misappropriation;
- Statutory remedies under applicable intellectual property, trade secret, and computer fraud laws; and
- Account of profits in equity and all other relief available under applicable law.

14.2 Equitable Relief

Reeseure may seek injunctive or equitable relief where monetary remedies would be inadequate to prevent or remedy the breach. Courts retain discretion in accordance with applicable law.

14.3 Legal Fees

In any enforcement action arising from User's material breach of these Additional Terms, User shall reimburse Reeseure for all reasonable legal fees, expert fees, and enforcement costs incurred.

15. SURVIVAL & GENERAL PROVISIONS

15.1 Survival — IP Provisions

The following provisions of these Additional Terms survive termination or expiry of the Agreement:

- Sections 2 (Patent Portfolio), 3 (Trade Secrets), 4 (Reverse Engineering), 5 (AI Training), 7 (Competitive Use) — indefinitely, to the maximum extent permitted by applicable law
- Section 8 (Non-Circumvention) — for the stated twenty-four (24) month period
- Section 10 (Feedback Licence) — perpetually
- Section 12 (Confidential Information) — as per the Terms of Service
- Section 14 (Remedies) — perpetually

Platform IP ownership, Patent Portfolio rights, trade secret protections, AI training prohibitions, reverse engineering restrictions, and non-circumvention obligations survive termination indefinitely to the maximum extent permitted by applicable law.

15.2 Relationship to Terms of Service

These Additional Terms are incorporated into and form part of the Agreement. In the event of any inconsistency with the Terms of Service with respect to intellectual property, trade secrets, reverse engineering, or non-circumvention, these Additional Terms prevail.

15.3 Severability

If any provision is held invalid or unenforceable, it shall be modified to the minimum extent necessary. If any prohibition is held unenforceable in its full scope, the narrowest enforceable scope shall apply.

15.4 Governing Law & Dispute Resolution

These Additional Terms are governed by the laws of India. All disputes shall be resolved by arbitration seated at GIFT City, Gujarat, India, in accordance with the dispute resolution provisions of the Reesecure Terms of Service.

CONTACT FOR IP ENFORCEMENT

For intellectual property enforcement and legal compliance inquiries:

Reesecure Group (Reesecure Pte. Ltd. and Reesecure IFSC Private Limited)

Email: office@reesecure.com

Regulatory entity: Reesecure IFSC Private Limited, GIFT City, Gandhinagar, Gujarat, India

Asia Pacific: Reesecure Pte. Ltd., Singapore