

# Kleene

## ACCEPTABLE USE POLICY

This acceptable use policy (the "**Policy**") sets out the rules governing Kleene services including data warehouse services and AI-powered services (the "**Services**") and the transmission, storage and processing of data and other content by means of the Services (the "**Data**").

Other Kleene legal documents referenced in this Policy, which also apply to customer use of the Services, are set out in the following table.

<b>Subscription T&amp;Cs</b>	Terms and conditions for Kleene's cloud-based software subscription services	<a href="https://kleene.ai/legal/subscription-tandcs">https://kleene.ai/legal/subscription-tandcs</a>
<b>Professional Services T&amp;Cs</b>	Terms and conditions for Kleene's professional services	<a href="https://kleene.ai/legal/professional-services-tandcs">https://kleene.ai/legal/professional-services-tandcs</a>

References in this Policy to "**you**" are to any customer for the Services under the Subscription T&Cs and/or the Professional Services T&Cs and any individual user of the Services (and "**your**" should be construed accordingly); and references in this Policy to "**us**" are to Minoro Limited (and "**we**" and "**our**" should be construed accordingly).

By using the Services, you agree to the rules set out in this Policy; in addition, we may require that you expressly agree to the rules set out in this Policy before using the Services.

Words in this Policy placing an obligation on you to refrain from doing an act, matter or thing include an obligation not to attempt to do that act, matter or thing, or instruct, authorise, permit or enable any other person to do or attempt to do that act, matter or thing.

### 1. Fair use

1.1 You must not use the Services or the Services infrastructure in a manner that results in excessive, unreasonable, abnormal or disproportionate:

(a) resource consumption, including consumption of compute, storage, memory, internal data transfer, data egress or data ingress resources;  
or

(b) cost or expenses being incurred by us,

in each case taking into account our relevant customer's historic usage.

1.2 The following shall apply from the fourth calendar month of a customer contract, and shall apply without prejudice to the foregoing. If the use of the Services, by or on behalf a Kleene customer, results in the third party costs or

expenses incurred by us during a calendar month with respect to that customer increasing by 100% or more as compared to the average of the third party costs and expenses incurred by us during the preceding 3 calendar months with respect to that customer, that shall be deemed to constitute a breach of this Policy. We shall give to the customer written notice of any such breach.

- 1.3 You must not use the Services in any way that causes, or may cause, damage to the Services or impairment of the availability, integrity, performance or accessibility of the Services.
- 1.4 You must not interfere with the use of the Services by our other customers.
- 1.5 You must not use the Services in any way that is not envisaged in the documentation for those Services.
- 1.6 You must not use the Services by means of any bot or other automated means, except through our public application programming interfaces or with our express written permission.
- 1.7 You must not sub-license your rights to use the Services or permit any unauthorised person or software to access or use the Services.
- 1.8 You must not:
  - (a) resell the Services or otherwise monetise the Services;
  - (b) use the Services to provide a bureau service to any other person; or
  - (c) integrate the Services with any other services,save to the extent that we have expressly authorised you to do so under a written reseller agreement or other written agreement.

## **2. Lawful use**

- 2.1 You must not use the Services:
  - (a) in any way that is unlawful, illegal, fraudulent, deceptive or harmful; or
  - (b) in connection with any unlawful, illegal, fraudulent, deceptive or harmful purpose or activity.
- 2.2 You must ensure that the Data is not illegal or unlawful, does not infringe any person's legal rights, and is not capable of giving rise to legal action against us or you or any other person (in each case in any jurisdiction and under any applicable law).
- 2.3 You must ensure that the Data is not and has never been the subject of any threatened or actual legal proceedings or any other similar complaint.
- 2.4 You must not use the Services in any way that breaches, or is liable to put us in breach of, any order or other requirement of any governmental authority.

- 2.5 You must comply with all export and import laws and regulations of the US, UK and other applicable jurisdictions in relation to your use of the Services.
- 2.6 You must not use the Services in any way that breaches, or is liable to put us in breach of, any terms and conditions applicable to the services that are integrated with the Services or upon which the Services depend.
- 2.7 The Data must not include any protected health information ("**PHI**") as that term is defined in the US Health Insurance Portability and Accountability Act ("**HIPAA**"), as amended and supplemented, unless you are the covered entity (as that term is defined in HIPAA) of such PHI.
- 2.8 The Data must not include any information that is controlled under the US International Traffic in Arms Regulations.

### **3. Security**

- 3.1 You must not conduct any profiling or performance testing (including load testing) on or using the Services without our prior written consent.
- 3.2 You must not conduct any vulnerability scans, penetration testing or other security testing on or using the Services without our prior written consent.
- 3.3 You must not circumvent any security measures of the Services.
- 3.4 You must not access any system, data, or account of the Services unless you have express authorisation for such access.
- 3.5 You must ensure that the Data does not contain or consist of, and you must not promote, distribute or execute by means of the Services:
  - (a) any viruses, worms, spyware, adware or other harmful or malicious software, programs, routines, applications or technologies; or
  - (b) any software, programs, routines, applications or technologies that will or may have a material negative effect upon the performance of a computer or introduce material security risks to a computer.
- 3.6 You must not reverse-engineer, decompile, or otherwise discover the underlying components, algorithms, source code, or proprietary models of the Services.
- 3.7 You must use the Services in compliance with any reasonable cyber and information security policies and procedures that we may notify to you from time to time.
- 3.8 Without prejudice to the foregoing, you must implement reasonable security measures to prevent unauthorised access to the Services via your credentials, systems, or integrations, including multi-factor authentication where supported.

## **4. Artificial intelligence**

- 4.1 You must not submit prompts, instructions, or inputs to our artificial intelligence-powered Services that:
- (a) are designed to, or are reasonably likely to: damage, corrupt, delete, or compromise the integrity of any data, databases, or system configurations; generate outputs that would cause system failures, performance degradation, or service interruptions; create security vulnerabilities or bypass authentication, access controls, or other protective measures; or execute resource-intensive operations that materially degrade service availability for other users;
  - (b) seek to generate, process, or facilitate: content that infringes third-party intellectual property rights; deepfakes or defamatory, fraudulent or deceptive content; content that violates data protection laws or processes personal data unlawfully; or content that breaches export control, sanctions, or other applicable legal restrictions; or code designed for harmful activities;
  - (c) attempt to: jailbreak reverse engineer, probe, or test the vulnerabilities of the Services or underlying infrastructure; extract training data, model parameters, or proprietary algorithms; generate outputs designed to exploit, harm, or deceive third parties; circumvent usage limits, content filters, or other restrictions; or
  - (d) request outputs that would or are liable to breach the terms of this Policy relating to the Data.
- 4.2 You must not use AI-generated outputs without appropriate human oversight and independent verification, including for: safety-critical systems or decisions; medical diagnosis, treatment, or health advice; legal advice or document preparation without qualified professional review; financial advice, credit decisions, or automated trading; or employment decisions, performance evaluations, or disciplinary actions.
- 4.3 You must not use the Services to create, develop, train, fine-tune, test, validate, maintain or update any machine learning or artificial intelligence model, software or system.
- 4.4 You acknowledge the Subscription T&Cs limit our liability with respect to artificial intelligence-generated outputs.

## **5. Monitoring and Breaches of this Policy**

- 5.1 We may monitor your use of the Services.
- 5.2 If you become aware of any breach of this Policy, you must promptly notify us in writing.
- 5.3 If you are or are acting on behalf of a Kleene customer, any breach of this Policy will be deemed to be a material breach of the contract between us and

the customer with respect to the relevant Services, and we may take such actions are permitted by the Subscription T&Cs in relation to any breach.

## **6. Variation**

6.1 This Policy may be varied:

- (a) with respect to non-customers, by us, updating the Policy as published on the Kleene website or through the Services; or
- (b) with respect Kleene customers, in accordance with the provisions of the Subscription T&Cs and/or Professional Services T&Cs as applicable between Kleene and the relevant customer.