POLICIES

Acceptable Use Policy

Last updated: August 24, 2026 · v1.0

Document Details

Provider: Develab Pte. Ltd., 10 Anson Road #10-11 International Plaza, Singapore (079903), UEN Ref. 202402923E

Products: Rideum Suite — Bleustay, Bleudine and Bleudash

Version: 1.0 · Effective 24 August 2026

Scope

This AUP applies to every user, customer, reseller, administrator, integration and automated process accessing any part of the Rideum Suite. It is incorporated into the End-User Agreement and each Order.

This Acceptable Use Policy (“AUP”) protects users, guests, merchants, hospitality customers, third parties and the security and availability of the Rideum Suite. Capitalised terms not defined here have the meanings in the Rideum Suite End-User Licence and SaaS Subscription Agreement (“End-User Agreement”). Customer is responsible for violations by its Authorised Users and anyone accessing the Services through its accounts, credentials, systems or integrations.

1. Lawful and authorised use

1.1 Permitted purpose. Use the Rideum Suite only for the internal business purposes, modules, properties, outlets, rooms, users, transactions, storage, API calls and other limits authorised by an Order and Documentation.

1.2 Law compliance. Do not use the Services for unlawful, fraudulent, deceptive, harmful or abusive activity, or in violation of privacy, consumer, payment, intellectual-property, communications, hospitality, tax, sanctions or export-control laws.

1.3 Authority over data. Do not submit, access, alter, disclose, export or delete data unless you are authorised by the relevant customer and have a lawful basis. Do not use the Services to obtain or infer information about another customer, guest, employee or user without authority.

2. Security and platform integrity

You must not:

Probe, scan, test or exploit vulnerabilities, or conduct penetration testing, red-team activity or security research without Provider's prior written authorisation.

Circumvent authentication, authorisation, billing, subscription, rate-limit, tenant-isolation, logging, anti-fraud, security or metering controls.

Access accounts, credentials, tokens, keys, systems, environments, interfaces or data that you are not expressly authorised to access.

Introduce malware, ransomware, spyware, malicious code, corrupted files, harmful scripts or content designed to disrupt, damage, monitor or gain unauthorised access.

Interfere with, overload, degrade or disrupt the Services, networks or another user, including denial-of-service activity, excessive queries or abusive automated traffic.

Share user accounts; expose passwords, API keys or tokens; disable required security settings; or fail to revoke access when a user no longer needs it.

Attempt to evade detection, conceal origin, falsify headers, impersonate another person or organisation, or use compromised credentials.

Publish vulnerabilities or security-test results before Provider has authorised disclosure and had a reasonable opportunity to remediate.

3. Intellectual property and misuse of the Services

You must not:

- Copy, modify, translate, adapt or create derivative works from the Services or Documentation except where expressly authorised.
- Reverse engineer, decompile, disassemble or attempt to discover source code, non-public APIs, architecture, algorithms, models, prompts, model weights or underlying techniques.
- Scrape, crawl, harvest or bulk extract data or content except through authorised export features or documented APIs within applicable limits.
- Frame, mirror, republish, rent, lease, resell, sublicense, timeshare or provide service-bureau access unless an Order expressly authorises it.
- Remove, obscure or alter copyright, trademark, attribution or proprietary notices.
- Use the Services, Documentation, outputs or non-public information to create, train, improve or benchmark a competing product or service.
- Publish benchmarks, performance tests, comparative reviews or security assessments containing non-public results without written approval.
- Upload or distribute content that infringes or misappropriates intellectual-property, privacy, publicity or other third-party rights.

4. Prohibited content and communications

Do not use the Services to create, store, display, transmit or facilitate:

- Content or activity that is illegal, fraudulent, deceptive, defamatory, threatening, harassing, hateful, discriminatory or intended to exploit or endanger a person.
- Child sexual abuse material, sexual exploitation, trafficking, non-consensual intimate material or content that unlawfully exposes minors.
- Spam, unsolicited bulk messaging, phishing, credential theft, misleading promotions or communications sent without required consent.
- Instructions, transactions or content intended to facilitate violence, terrorism, weapons offences, money laundering or other serious crime.
- False bookings, transactions, reviews, identities, rates, inventory, tax information, payment details or other manipulated business records.
- Personal data that is excessive for the stated purpose, prohibited by the Order, collected unlawfully or processed contrary to data-subject rights.
- Payment-card or authentication data in unapproved fields, logs, support tickets or free-text areas where Provider has not expressly designed the Service to receive it.

5. Hospitality, commerce and operational safeguards

5.1 Accuracy and review. Users must review rates, availability, bookings, menus, orders, taxes, payments, dashboards, reports, automated recommendations and guest communications before relying on them. Do not intentionally publish false, deceptive or unlawful information.

5.2 Guest and employee data. Access guest, visitor, staff and applicant data only for authorised operational purposes. Apply least privilege, avoid unnecessary sensitive data, and do not use such data for personal purposes, surveillance, discrimination, harassment or unauthorised marketing.

5.3 Payments. Do not use the Services to process stolen instruments, launder funds, evade chargebacks, misrepresent transactions, split transactions to avoid controls or violate payment-provider rules. Use only approved payment interfaces and never store prohibited card authentication data.

5.4 Automated outputs. Do not treat dashboards, analytics, forecasts, recommendations or AI-assisted outputs as infallible. Users must exercise human review appropriate to the impact, especially for pricing, guest treatment, employment, credit, safety, legal or other significant decisions.

5.5 Integrations and APIs. Use APIs and integrations only as documented. Observe rate limits, authentication and data minimisation; secure tokens; do not cache data longer than necessary; and stop access when authority ends. Customer is responsible for its integration code and third-party services.

6. Resource limits and fair use

6.1 Limits. Do not exceed purchased metrics or use technical workarounds to avoid fees, storage limits, transaction limits or subscription restrictions. Provider may measure consumption and require an upgrade, throttle activity or charge excess use under the Order.

6.2 Excessive use. Activity is excessive if it materially degrades the Services, creates disproportionate cost or risk, interferes with others or departs materially from ordinary use for the purchased plan. Provider may request remediation and impose reasonable technical limits.

6.3 Automation. Bots, scripts, bulk operations and machine-to-machine access are permitted only through documented functionality or APIs and must respect concurrency, volume and rate limits. Attempts to rotate accounts, IP addresses or credentials to evade limits are prohibited.

7. Account and security responsibilities

7.1 Credentials. Keep credentials confidential, use unique passwords and multi-factor authentication where available, and do not allow shared or generic user accounts except approved service accounts. Notify Provider immediately of loss, compromise or unauthorised use.

7.2 Access management. Review users and privileges regularly, promptly disable inactive or departed users, separate administrative duties where appropriate, and restrict exports and sensitive functions to authorised personnel.

7.3 Systems and devices. Use supported, patched and reasonably secured devices, browsers, networks and integration systems. Do not access administrative functions from public or untrusted devices without appropriate safeguards.

8. Monitoring, reporting and cooperation

8.1 Monitoring. Provider may monitor metadata, usage, logs and content to the extent reasonably necessary to operate and secure the Services, verify compliance, investigate suspected abuse and satisfy legal obligations, subject to the Privacy Policy and DPA.

8.2 Reporting. Report suspected vulnerabilities, account compromise, unlawful content, data exposure or AUP violations promptly to sales@develab.io. Do not publicly disclose a vulnerability before Provider authorises coordinated disclosure.

8.3 Cooperation. Customer will preserve relevant evidence, provide accurate information, stop harmful activity, reset credentials, remove prohibited content and reasonably assist Provider's investigation, containment, notification and remediation.

8.4 No retaliation. Do not retaliate against a good-faith reporter. Provider may protect reporter confidentiality where lawful but does not promise anonymity.

9. Enforcement

9.1 Protective action. Provider may remove or restrict content, revoke tokens, throttle activity, block integrations, reset credentials, suspend accounts or Services, preserve evidence, notify affected customers or authorities where required, and take other proportionate action to prevent harm or comply with law.

9.2 Notice. Where practicable and safe, Provider will notify Customer of a suspected violation and allow a reasonable opportunity to cure. Immediate action may be taken for security threats, unlawful content, fraud, infringement, non-payment, serious privacy risk, sanctions exposure or likely harm.

9.3 Repeated or serious violations. Repeated, intentional or serious violations may result in termination under the End-User Agreement and may be referred to law enforcement or regulators where required or appropriate.

9.4 No liability for proper enforcement. To the maximum extent permitted by law, Provider is not liable for good-faith enforcement reasonably undertaken under this AUP. Customer remains responsible for fees and liabilities incurred before suspension or termination.

10. Changes and interpretation

10.1 Changes. Provider may update this AUP to address security, legal, product or abuse developments. Material changes will be notified in accordance with the End-User Agreement; urgent protective changes may take effect immediately where reasonably necessary.

10.2 Conflict. The End-User Agreement controls if it expressly conflicts with this AUP. This AUP does not reduce Customer's obligations under law, the Order, the DPA, payment-provider rules or third-party terms.

10.3 Questions. Questions and reports should be sent to sales@develab.io. Provider: Develab Pte. Ltd., 10 Anson Road #10-11 International Plaza, Singapore 079903 (UEN 202402923E).