TRAVEL CODE ACCEPTABLE USE POLICY

This Acceptable Use Policy is incorporated into the Travel Code Master Platform Agreement and applies to the Customer and to every User. Capitalized terms not defined here have the meaning given in the Master Agreement.

Travel Code may update this Policy in accordance with §14.4 of the Master Agreement.

---

1. WHO MAY USE THE PLATFORM

The Platform is for **business entities using it for bona fide commercial purposes**. It is not available to consumers, or to individuals or sole proprietors acting in a personal capacity.

---

2. RESTRICTED INDUSTRIES

The Customer may not use the Platform if it operates in, and may not use the Platform in connection with:

- weapons, firearms, ammunition, or military equipment;
- gambling, betting, gaming, or lotteries;
- adult entertainment or sexually oriented goods and services.

These restrictions are required by Travel Code's banking and card partners and are not waivable. Additional restrictions apply to the Card Program under Schedule C and under the Card Agreements.

The following require Travel Code's prior written approval before the Platform is used in connection with them: cryptocurrency and digital asset businesses; cannabis and cannabis-related businesses; money services businesses; debt collection; multi-level marketing; pharmaceuticals and controlled substances; precious metals and stones dealing.

---

3. PROHIBITED CONDUCT

The Customer and its Users must not:

3.1 Unlawful use. Use the Platform in violation of any applicable law, regulation, or card network rule; for money laundering, terrorist financing, tax evasion, fraud, or the concealment of proceeds of crime; or to evade sanctions.

3.2 Sanctions. Use the Platform for the benefit of any person or entity subject to sanctions

administered by the U.S. Office of Foreign Assets Control, or listed on any applicable restricted or denied party list, or located in a comprehensively sanctioned jurisdiction. Travel Code screens for this and will block or terminate accordingly.

3.3 Misrepresentation. Provide false, inaccurate, incomplete, or misleading information at onboarding or afterwards; impersonate another person or entity; or conceal beneficial ownership.

3.4 Personal use. Use corporate cards, travel booking, or expense functionality for personal, family, or household purposes.

3.5 Unauthorized access. Access or attempt to access any account, system, or data the Customer is not authorized to access; share credentials; or circumvent authentication, rate limits, or access controls.

3.6 Interference. Interfere with or disrupt the Platform or its infrastructure, including through denial-of-service activity, malware, or excessive automated requests.

3.7 Reverse engineering. Reverse engineer, decompile, disassemble, scrape, or attempt to derive the source code, structure, or underlying models of the Platform, or use the Platform to build or benchmark a competing product.

3.8 Data misuse. Upload data the Customer has no right to process; process the personal data of individuals who are not its Users; or use the Platform to send unsolicited bulk commercial communications.

3.9 Harmful content. Upload or transmit content that is unlawful, infringing, defamatory, harassing, or that contains malicious code.

3.10 Resale. Resell, sublicense, or provide the Platform to third parties on a service bureau or time-share basis, except as expressly permitted in a Service Order or in a separate written Partner Agreement with Travel Code.

3.11 Critical use. Use the Platform where failure could lead to death, personal injury, or environmental damage.

3.12 Card misuse. Where the Card Program applies, use cards other than as permitted by Schedule C and the Card Agreements, including any attempt to obtain cash other than as expressly enabled, to structure transactions, or to generate rewards through artificial, circular, or manipulative activity.

---

4. TRAVEL-SPECIFIC RESTRICTIONS

4.1 The Customer must not book travel for individuals subject to sanctions or restricted party listings.

4.2 The Customer must not use the Platform to book travel it knows or should know is for an unlawful purpose, or to circumvent immigration or border controls.

4.3 The Customer is responsible for ensuring its travellers hold valid documentation and comply with the requirements of each destination.

4.4 The Customer must not exploit supplier pricing errors, engage in speculative or fictitious booking, hidden-city or throwaway ticketing, or any practice prohibited by a supplier's fare rules.

---

5. ENFORCEMENT

5.1 Travel Code may investigate suspected breaches and may suspend or restrict access to the Platform, to a specific feature, or to an individual User's account.

5.2 Travel Code may act **immediately and without prior notice** where it reasonably believes there is a risk of unlawful activity, fraud, harm to another customer, harm to the Platform, or breach of a requirement imposed by a regulator, a card network, the issuing bank, or the card program manager.

5.3 Suspension does not relieve the Customer of accrued payment obligations. Repeated or material breach is grounds for termination for cause under §12.3 of the Master Agreement.

5.4 The Customer is responsible for its Users' compliance with this Policy and must notify Travel Code promptly of any suspected breach.

---

6. REPORTING

Report suspected misuse, security issues, or vulnerabilities to **security@travel-code.com**.