# Acceptable Use Policy (AUP)

This Acceptable Use Policy applies to all Services supplied by Vetta Trading Limited (Vetta) and forms part of the Agreement between Vetta and the Customer.

The Customer is responsible for ensuring that all users of the Services, including employees, contractors, agents and end users, comply with this AUP.

**1. Purpose of this Policy**

1.1 This AUP is designed to:
(a) protect Vetta's network, systems and Services
(b) ensure fair and lawful use by all users
(c) maintain service quality and integrity
(d) prevent harm, misuse, fraud or illegal activity.

**2. Prohibited Activities**

The Customer must not use the Services, and must not allow others to use the Services, for any activity that:

2.1 Breaks the law, including but not limited to:
(a) accessing, possessing, transmitting or distributing objectionable or illegal content
(b) infringing copyright or intellectual property rights
(c) breaching privacy laws
(d) breaching the Harmful Digital Communications Act
(e) unauthorised access to computer systems (hacking)

2.2 Harms Vetta's network or other networks, including:
(a) attempting to probe, scan, penetrate or test the vulnerability of any system
(b) distributing malware, ransomware, viruses or malicious code
(c) running open relays, open proxies or open resolvers
(d) launching or participating in denial-of-service attacks

2.3 Is abusive, fraudulent or malicious, including:
(a) phishing, impersonation or social engineering
(b) fraud, scams or payment-related deception
(c) harassment, bullying, defamation or threats
(d) distribution of harmful, offensive or abusive content

2.4 Interferes with service delivery, including:
(a) tampering with or misusing Vetta or LFC Equipment
(b) circumventing traffic management or security controls
(c) performing actions that degrade network performance for others.

**3. Email, Messaging and Spam Restrictions**

3.1 The Customer must not send:
(a) unsolicited bulk messages (spam)
(b) commercial electronic messages that breach anti-spam laws
(c) email with forged headers or deceptive addressing
(d) malware or harmful attachments

3.2 Vetta may block or filter traffic suspected to be spam or malicious.

**4. Voice Services and VoIP Restrictions**

For any telephony, SIP, PBX or VoIP Services, the Customer must not:

4.1 Use autodialers, predictive dialers, bulk calling systems, war dialers or high-volume automated call generation tools unless explicitly approved in writing.

4.2 Make or attempt to make calls for fraudulent or high-risk purposes, including:
(a) international toll fraud
(b) calling high-risk destinations repeatedly
(c) artificially inflating traffic

4.3 Attempt to manipulate CLI, caller identity, call routing or billing records.

4.4 Interconnect Vetta's voice service to any third-party carrier or network without permission.

**5. Security Requirements**

The Customer must:

5.1 Maintain the security of all devices, endpoints, applications, passwords and access credentials.

5.2 Use up-to-date antivirus, anti-malware, patches and updates on connected systems.

5.3 Not expose insecure or misconfigured systems to Vetta's network.

5.4 Notify Vetta immediately if:
(a) a security breach occurs
(b) credentials are compromised
(c) unauthorised access is suspected
(d) malware infection is detected on systems using the Service.

**6. Fair Use**

6.1 Some Services (including "unlimited" and "uncapped" plans) are subject to Fair Use requirements to ensure service quality for all customers.

6.2 Fair Use means usage that is:
(a) reasonable and proportionate to typical customer usage
(b) not excessive compared to other users of the same plan
(c) not affecting Vetta's ability to deliver Services to others.

6.3 If Vetta identifies excessive or unreasonable usage, Vetta may:
(a) contact the Customer to discuss usage
(b) apply traffic management or shaping
(c) require the Customer to move to a different plan
(d) suspend or limit the Service in severe cases.

**7. Hosting, Cloud and IT Services**

For hosted services, cloud services or managed IT services, the Customer must not:

7.1 Host illegal, harmful, infringing or objectionable content.

7.2 Run cryptocurrency mining, high-intensity compute workloads or resource-abusive processes without written approval.

7.3 Use Vetta's infrastructure to deliver competing wholesale services unless explicitly authorised.

**8. Payments and EFTPOS Services**

For payments-related services, the Customer must:

8.1 Comply with all PCI DSS requirements applicable to their environment.

8.2 Not store, process or transmit cardholder data in violation of PCI DSS.

8.3 Immediately notify Vetta of any suspected compromise of payments systems.

**9. Network Usage and Performance Management**

9.1 Vetta may implement network management practices to:
(a) maintain network performance
(b) prevent congestion
(c) protect security
(d) ensure Fair Use.

9.2 These may include shaping, filtering, rate limiting, traffic prioritisation or blocking malicious traffic.

**10. Enforcement**

10.1 Vetta may take any reasonable action to enforce this AUP, including:
(a) contacting the Customer to request corrective action
(b) issuing warnings
(c) suspending or restricting the Service
(d) terminating the Service in serious or repeated cases

(e) blocking or filtering harmful or malicious traffic.

10.2 The Customer remains liable for all Charges during any suspension unless caused by Vetta's breach.

10.3 Vetta may report illegal activity to law enforcement agencies.

**11. Changes to this Policy**

Vetta may update this AUP from time to time by providing written notice or publishing the updated version on its website. Continued use of the Services constitutes acceptance of the amended policy.