Information Security

Information Security

Last updated: 9 March 2023

1. Information Security

1.1 TradingHub shall have a documented information security policy which is reviewed at least annually and shall implement and maintain supporting processes and procedures.

1.2 TradingHub shall implement and maintain administrative, technical and physical security measures designed to ensure the confidentiality, integrity and availability of, and to prevent unauthorised access to or use of, the Customer's confidential information. Such measures shall be based on industry best practices and recognised security standards.

1.3 TradingHub's production hardware infrastructure is currently provided by Amazon Web Services ("**AWS**") and is designed and managed in alignment with security best practices and a variety of IT security standards, including:

- SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70)
- SOC 2
- SOC 3
- FISMA, DIACAP, and FedRAMP
- DOD CSM Levels 1-5
- PCI DSS Level 1
- ISO 9001 / ISO 27001
- ITAR
- FIPS 140-2
- MTCS Level 3

1.4 TradingHub's security measures shall include regular monitoring and penetration testing of the Services (also known as vulnerability threat assessments and vulnerability scanning) by an information security company with ISO 27001 accreditation. TradingHub shall take commercially reasonable efforts to remediate any issues identified by such penetration testing as "critical" or "high" prior to implementation in the Services and to promptly remediate any other material security defects in the Services of which TradingHub becomes aware.

1.5 At the reasonable request of the Customer, TradingHub shall provide to Customer a copy of its most recent application and IT infrastructure penetration testing report and its third party cloud provider's published report on Certifications, Programs, Reports and Third-Party Attestations (or similar documentation). TradingHub shall reasonably cooperate with any reasonable request by Customer for updated information regarding TradingHub's information security measures with respect to the Services.

1.6 TradingHub shall use such controls as are reasonable and appropriate (as determined by TradingHub) to protect against unauthorised access to the Services, including use

of a secured network connection to transmit confidential information between TradingHub and Customer, data encryption in transit and at rest and, if requested by the Customer and subject to payment of additional fees, multifactor authentication.

1.7 The Services shall include user access log viewing capabilities and history information covering user access and user actions during the term of the Contract. TradingHub shall restrict external access to the Services to Customer provided whitelisted IP addresses. Any changes to such whitelist may only be requested by nominated staff of the Customer.

1.8 TradingHub's physical and software security measures shall include the use of physical access and intrusion detection controls, secure off-site backup and appropriate firewalls and virus detection software designed to prevent unauthorised access to Confidential Information. Except where otherwise provided in the Contract, TradingHub shall at all times logically segregate Customer Trade Data from the trade data of other customers of TradingHub.

1.9 TradingHub shall ensure that it has carried out pre-employment screening checks on its employees having access to confidential information of the Customer. Such pre-employment screening shall include identity check, international credit check (where appropriate), international criminal check (where appropriate), national criminal check (where appropriate), verification of highest level of education, electoral role check and 5 year employment history check.

2. Business continuity

TradingHub shall have a documented business continuity plan which is reviewed and tested at least annually.