Information Security

Last Reviewed: 22 April 2024

1. APPLICABILITY

This information security schedule ("**ISS**") will govern the provision and use of the Services provided it is explicitly incorporated into the Contract by reference. Where the ISS applies, in the event of a conflict between the terms of the ISS and the terms of the Contract, the terms and conditions of this ISS take precedence, but only to the extent of such conflict. Capitalised terms used herein but not defined herein shall have the meanings set forth in the Contract.

2. DEFINITIONS

"**Applicable Data Protection Legislation**" means:
(a) to the extent the UK GDPR applies, the law of the United Kingdom or of a part of the United Kingdom
which relates to the protection of personal data, including: (i) UK GPDR; (ii) the Data Protection Act 2018; (iii) the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC); and (iv) the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) (in each case as amended from time to time); and
(b) to the extent the EU GDPR applies, the law of the European Union or any member state of the European Union to which TH is subject, which relates to the protection of personal data;

"**Contract**" means the contract for services between the Customer and TH;

"**Customer**" means the entity you represent, which has entered into a contract for services with TH;

"**Customer Confidential Information**" in relation to the Customer, means all of confidential or proprietary nature, disclosed or contained in any form and howsoever provided, including but not limited to information or other materials relating to:

(a) The business, client or financial or other affairs;
(b) Any information or other materials expressly indicated by the Customer as confidential at the time of disclosure;
(c) Trade secrets, know-how, systems, programs and products and other proprietary confidential, technical or commercial information and materials;
(d) Personnel, agents, third party intermediaries and suppliers;
(e) future projects, business development or planning, commercial relationships and negotiations;
(f) anything a reasonable businessperson could reasonably be expected to know is confidential,

in each case existing in any form, whether or not marked "confidential information" and all other information clearly designated by the disclosing party as confidential;

"**EU GDPR**" means the General Data Protection Regulation ((EU) 2016/679);

"**Personal Data**" shall have the meaning ascribed to it in the Applicable Data Protection Legislation;

"**Trade Data**" means the raw trade, order and/or positions data provided by Customer (or a Customer Affiliate as applicable) to TradingHub, which relates to the Covered Asset Classes and Covered Entities specified within relevant Contract , to enable TradingHub to provide the Services;

"**Secure Software Development Lifecycle**" means a framework for integrating security into the software development lifecycle in order to develop secure software;

"**Services**" means the services to be provided by TradingHub as set out in the relevant Contract;

"**UK GDPR**" has the meaning given to it in the Data Protection Act 2018;

3. INFORMATION SECURITY

3.1. Documentation

(a) TradingHub maintains documented security processes and plans which ensure the confidentiality, availability, and integrity of Customer Confidential Information in accordance with industry best practices, including ISO/IEC 27001:2022 and SOC2.
(b) TradingHub's Policies and Standards are reviewed and updated at least annually.
(c) TradingHub maintains an up-to-date asset register of information technology assets.

3.2. Hosting location

(a) Trade Data is hosted by a third-party cloud provider and each customer's data is segregated to its own environment which prevents it from comingling with data from other customers/sources.

3.3. Training and awareness

(a) TradingHub ensures that all employees complete Information Security training on an annual basis, covering areas such as social engineering, phishing, secure remote working, fraud and managing online risks. New employees must complete their assigned training upon joining.
(b) TradingHub enforces a clear desk and clear screen policy. Screens are configured to automatically lock after a period of inactivity no longer than 10 minutes.
(c) All staff are required to read and accept the TradingHub Acceptable Use Policy which includes but is not limited to the acceptable use of company equipment and email and details prohibited activities.

3.4. Background Screening

(a) Background and reference checks are performed on all employees prior to their employment.
(b) Background screening checks include the following:
- ID verification
- Basic criminal record check
- Employment history
- Gap analysis
- Highest education verification
- Professional memberships

3.5. **Secure Software Development Lifecycle**

(a) TradingHub maintains documentation for Secure Software Development Lifecycle that sets out the expectations and requirements regarding secure development of applications and maintenance process.
(b) TradingHub maintains fully segregated development, test, and production environments.
(c) Customer data is strictly prohibited from being introduced into non-production environments.
(d) TradingHub implements controls to ensure the protection of source code including backups and version control.
(e) TradingHub code is reviewed and tested during development including source code reviews and regression testing.
(f) All code changes go through four eyes review and are tested in non-production environments prior to deployment.
(g) Sample programs, test code, scripts or test pages are not deployed to production systems.
(h) Source code shall not contain hard coded credentials or any other secret material.
(i) Appropriate restrictions are in place to ensure segregation of duties across critical functions.

3.6. **TH Staff Access Management**

(a) TradingHub maintains robust processes to ensure that access to the Trade Data under its control is restricted to those individuals who are explicitly authorised to access such data.
(b) Access shall be provisioned based on the principle of least privilege granting only the minimum privileges appropriate to perform the required job functions.
(c) Staff account passwords must meet the following enforced complexity requirements:
    - Minimum of 12 characters
    - Unable to reuse any of the 20 most recently used passwords
    - Contain three out of four of the following:
        - Lowercase characters
        - Uppercase characters
        - Numbers (0-9)
        - Symbols
(d) Access shall be assigned using unique logon credentials to ensure accountability is maintained.
(e) Strong authentication methods (including multi-factor authentication) for those of its personnel who work remotely and for those with TradingHub administrative privileges upon systems used to provide the Services.
(f) Access to production systems shall only be achieved via a break glass mechanism following approval.
(g) Privileged accounts undergo periodic review at least quarterly.
(h) TradingHub staff accounts that are inactive for 90 consecutive days are disabled.
(i) Root accounts for cloud services are secured by a hardware security token providing multi-factor authentication.

3.7. **Customer Access Management**

(a) Where the Customer has additional access control requirements, such as multi-factor authentication, TradingHub supports Single-Sign On (SSO) integration enabling the Customer to manage this through the Customer's Identity Provider.
(b) SFTP credentials are provided directly by TradingHub to an authorized person assigned by the Customer as part of onboarding. Maintaining security of these credentials is a responsibility of the Customer.

(c) Customer user sessions are automatically terminated after a maximum of 60 minutes of inactivity and can only be re-established by re-authenticating.
(d) Environments provisioned to deliver services to the Customer are IP whitelisted to the Customer's corporate IP addresses to restrict access to known and trusted locations only. It is the Customer's responsibility to ensure they provide TradingHub with a complete list of CIDR ranges for their corporate outbound web proxy.

3.8. **Vulnerability Management and Security testing**

(a) TradingHub regularly scans its networks and systems for vulnerabilities and security issues.
(b) Network Penetration tests and Application Penetration tests are performed at least every 12 months by an external specialist company. Customer is prohibited from conducting their own network penetration tests.
(c) Customers are prohibited from conducting their own application penetration tests unless prior permission has been granted. If permission is granted, the Customer's application penetration tests must be completed in a non-production environment, and results of the penetration tests must be shared with TradingHub.
(d) A threat detection system continuously monitors the cloud environment to detect anomalies and suspicious activities.
(e) Findings raised from security testing and scans are prioritised based on the severity and associated risk posed by the issues identified within timeframes defined in TradingHub's Vulnerability Management Standard.
(f) A patch management process is in place which ensures patches are appropriately tested and promptly deployed to rectify security vulnerabilities.

3.9. **Encryption**

(a) Encryption technologies are in place to protect the Trade Data during transmission and storage and, where appropriate, the pseudonymisation of the data.
(b) Only secure protocols, algorithms, and key lengths recognised as industry standard are used.
    - A minimum of TLS 1.2 for data in transit
    - A minimum of AES256 for data at rest
(c) Encryption protocols, algorithms, or key lengths deemed end of life are strictly prohibited.
(d) Cryptographic keys are securely stored within a Key Management Service (KMS) using industry certified shared Hardware Security Modules (HSM).

3.10. **Certificate Management**

(a) A centralised certificate management system is used to provision and manage certificates for secure communication.
(b) Certificates used for production environments are issued from a trusted third-party Certificate Authority recognised within the industry for their reliability and security standards.
(c) Certificates employed in production environments shall have a single and clearly defined purpose, whether it be for digital signatures, encryption, or any other specified purpose.

3.11. **Business Continuity and Disaster Recovery**

(a) TradingHub applies reasonable measures to maintain continuity of Services, as well as measures to restore the availability and access to Trade Data in a timely manner in the event of a physical or technical incident.
(b) TradingHub maintains written Business Continuity and Disaster Recovery plans.
(c) Business Continuity and Disaster Recovery scenarios are tested at least annually.

3.12. **Incident Response**

(a) TradingHub maintains a documented Incident Response Standard to ensure incidents are appropriately managed and analysed to avoid re-occurrence and determine lessons learned.

3.13. **Physical security**

(a) To guarantee safety of employees and visitors and to protect the property of TradingHub, the office facilities are equipped with fire alarms and fire extinguishers and other safety and security features as required by local safety regulations.

(b) All entry and exit points, server rooms and spaces with restricted access within the TradingHub premises are subject to constant electronic monitoring through CCTV to prevent and detect any crime or unlawful activities on the premises.

(c) All entry points are controlled by an electronic access control system.

3.14. **Security Breach**

(a) Subject to paragraph 3.14.(b) below, TradingHub will, to the extent permitted by law, notify the Customer promptly, if it becomes aware of, or reasonably suspects, any breach of TradingHub's security leading to the unlawful destruction, loss, alteration, or access to Customer Confidential Information (a "**Security Breach**"). TradingHub will work with the Customer's Incident Response team until the incident is closed, including providing a post-mortem document to the Customer once all details are known.

(b) Notwithstanding paragraph 3.14.(a) above, where a Security Breach involves Customer Personal Data, notification of such breach will be dealt with under the relevant terms of the Contract and paragraph 3.14.(a) above shall not apply.

3.15. **Network & System Security**

(a) TradingHub ensures mechanisms are in place to prevent the unauthorised removal or disclosure of Trade Data from its networks via technologies such as removable media, the internet, email, or instant messaging services.

(b) Systems are synchronised to a Network Time Protocol (NTP) service.

(c) Controls are implemented and maintained to ensure the integrity and confidentiality of production and non-production networks including but not limited to network access controls, intrusion detection/prevention, virtual firewalls, and segregated environments.

(d) Processes have been established to continually monitor TradingHub networks and systems for potential or actual Security Breaches.

(e) Up-to-date anti-virus and anti-malware software is deployed and configured in line with industry security standards.

(f) Anti-phishing and anti-spam email scanning in place with automatic quarantine of suspicious emails.

(g) TradingHub ensures necessary steps are taken to ensure that no malware is introduced onto the Customer systems by any TradingHub employee or third party acting on behalf of TradingHub.

(h) TradingHub provided portable devices are centrally managed and configured with full disk encryption and blocking of removable media enforced.

3.16. **Logging and monitoring**

(a) Systems are configured to write security audit information to logs and procedures in place for the analysis and handling of logs, aligned with the security standards.

(b) Access to logs is restricted to authorised individuals and protected against modification and tampering.

(c) Tools are employed to monitor, collect, and analyse security logs for security events.

3.17 **Record retention**

(a) Unless otherwise specified in the Contract, TradingHub retains Customer Confidential Information for the period as specified within TradingHub's Record Retention policy. Beyond the retention period, the cloud provider securely destroys Customer data using best practice industry standard techniques.

3.18 **Change Management**

(a) TradingHub has established robust processes to ensure that changes to the premises, networks, systems, software, information, websites, and other media used to supply TradingHub services are appropriately tested and implemented to limit the potential for any adverse impact on the supply of the services.

(b) TradingHub will notify Customers within a timely manner of any changes in its environment that will have a negative material impact to the Services delivered.

3.19 **Third Parties**

(a) TradingHub conducts annual due diligence of critical third parties that directly support the delivery of TradingHub services to ensure appropriate security controls are in place that are consistent with the security requirements of this Information Security Schedule.

3.20 **Security Audit**

(a) TradingHub undergoes independent external security audits at least once annually in accordance with maintaining ISO/IEC 27001:2022 certification and SOC2 Type 2 annual attestation.

(b) Customers wishing to conduct a security audit or review of TradingHub are first directed towards TradingHub's Security Pack (available on request) which includes but is not limited to independent audit reports, penetration test results, disaster recovery test results, and an overview of TradingHub's security policies.

(c) Where a Customer requires to perform an audit of TradingHub, the audit shall not exceed elapsed time of five (5) business days within a twelve (12) month period unless otherwise specified within the Contract.

Legal disclaimer