QUANTECH SERVICES GROUP

QSG SaaS
Security Policy

This Security Policy describes the general security practices applicable to software-as-a-service products and related services made available by Quantech Services Group ("QSG", "we", "us", or "our"). Specific security measures may vary depending on the applicable SaaS product, service configuration, deployment model, and applicable subscription terms.

1. Encryption

QSG uses commercially reasonable and industry-standard measures to protect Client Data in transit and at rest, where applicable. Data in transit is generally protected using secure transport protocols, such as TLS or equivalent industry-standard encryption. Data at rest is protected using appropriate encryption or other technical safeguards based on the nature of the data, the applicable service architecture, and the relevant security requirements.

2. Tenant Isolation

QSG maintains logical, network-level, system-level, or other appropriate segregation measures designed to prevent unauthorized access between Client environments and Client Data. The specific isolation methods may vary depending on the applicable SaaS product, deployment model, and service configuration. QSG does not intentionally permit one Client to access another Client's data or environment unless expressly authorized by the relevant Client.

3. Authentication and Access Controls

QSG applies reasonable authentication and access-control measures before granting access to Client Data or applicable SaaS environments. Depending on the relevant SaaS product and configuration, such measures may include account verification, credential-based authentication, access approval procedures, role-based access controls, or other appropriate security controls.

4. Audit Logging

To the extent a SaaS product processes Client Data, QSG enables and retains system-generated audit logs of security-relevant events for at least one (1) year. Such logs are maintained using commercially reasonable safeguards designed to protect them against unauthorized alteration or tampering.

QSG may maintain audit logs through its own infrastructure, cloud service providers, infrastructure providers, or other service providers. Except as required by applicable law, QSG is not obligated to provide Clients with direct access to, copies of, or customized reports based on such audit logs.

5. Vulnerability Management

QSG maintains reasonable processes intended to identify and address material security vulnerabilities in the SaaS. These processes may include version management, security reviews, vulnerability assessments, scanning, monitoring, or other measures that QSG considers appropriate in light of the relevant SaaS product and its operating environment.

Where QSG identifies a material security vulnerability, QSG will assess and address the issue within a commercially reasonable timeframe, taking into account the nature, severity, exploitability, and operational impact of the issue.

6. Security Incident Notification

If QSG becomes aware of a security incident involving unauthorized access to, acquisition of, or disclosure of Client Data that is reasonably likely to materially affect a Client, QSG will notify the affected Client within a commercially reasonable timeframe, subject to applicable law and the information reasonably available to QSG at the time.

Unless otherwise agreed in writing, notifications will be sent to the contact details maintained in the applicable Client account or subscription records.

7. Security Incident Reporting

Clients may report a suspected security issue or security incident relating to a QSG SaaS product by contacting:

Email: contact@quantech.services
Subject: Security Concern

8. Data Handling Practices

QSG collects only such Client Data as is reasonably necessary to provide, operate, support, secure, and improve the applicable SaaS. Client Data is stored using appropriate technical and organizational safeguards, including encryption where applicable.QSG uses Client Data solely for the purposes of providing and maintaining the SaaS, complying with applicable legal obligations, and improving service performance.

Client Data is retained only for as long as reasonably necessary to provide the SaaS or satisfy applicable legal and contractual requirements. Client Data may be deleted in accordance with the applicable End User License Agreement, applicable subscription terms, or a valid Client request, subject to applicable laws, contractual requirements, and QSG's backup and retention procedures.