Security & Data Handling Overview

Prepared for InfoSec / IT Review

Document Version: 1.1 | Date: April 2026 | Classification: Confidential

Company Overview

Scalient IQ provides GTM (Go-To-Market) orchestration for mid-market B2B companies. Our platform, SiQ Cortex, connects to a client's existing CRM and revenue tools via API integrations to analyze buying signals, score pipeline health, and generate actionable recommendations for revenue teams.

SiQ engagements operate in two modes with distinct data-access profiles:

Assessment Mode (GTM Signal Assessment engagement): Strictly read-only. All OAuth scopes are read-only. SiQ cannot write, modify, or delete data in client systems.

Platform Mode (ongoing SiQ Cortex subscription): Read access plus optional, customer-authorized write-back capabilities. Any write action (e.g., CRM field updates, outbound communications) requires a separate OAuth grant with write scopes and passes through the HITL Approval Queue before execution. No write action fires without explicit human approval.

This document covers how we access, process, store, and protect client data across both engagement modes.

Connection Architecture

Item	Details
Authentication	OAuth 2.0 with PKCE (where supported). Standard vendor OAuth flows identical to HubSpot, Salesforce, Gong, Outreach integrations.
Access Level	Assessment engagement: Strictly read-only. All OAuth scopes are read-only; SiQ cannot write, modify, or delete data in client systems. Platform engagement: Read access plus optional write-back capabilities. Any write scope requires separate customer authorization and every write action passes through the HITL Approval Queue before execution.
Connection Method	REST API over TLS 1.2+ encrypted connections. No direct database access. No VPN tunnels. No agents or code installed in client environments.
Scope Transparency	Full list of OAuth scopes provided before authorization. Client reviews and approves each scope explicitly.
Revocation	Client can revoke API access at any time from their CRM admin panel. Revocation is immediate and requires no SiQ involvement.

Data Handling & Processing

Category	Policy
Data in Transit	All data transmitted over TLS 1.2+ encrypted connections. No unencrypted data transfer at any point.
Data at Rest	Encrypted using AES-256 at rest. All client data stored in isolated, logically separated environments.
Data Residency	Client data processed and stored within US-based cloud infrastructure (AWS). No cross-border data transfer without explicit client consent.
Data Retention	Assessment data retained for 90 days post-delivery for support purposes, then permanently deleted. Platform clients: data retained for duration of contract + 30-day grace period.
Data Deletion	Client can request full data deletion at any time. Deletion completed within 14 business days with written confirmation.
PII Handling	SiQ Cortex processes business contact records (name, email, title, company) as provided by the client's CRM. No consumer PII. No financial data. No health data.

Infrastructure & Security Controls

Control	Implementation
Cloud Provider	Amazon Web Services (AWS), US regions.
SOC 2 Alignment	Security controls aligned to SOC 2 Type II framework. Formal audit in progress.
Access Control	Role-based access (RBAC). All internal access requires MFA. Principle of least privilege enforced.
Logging & Monitoring	All API access logged with timestamps, user identity, and action type. Anomaly detection active on all client data endpoints.
Incident Response	Documented incident response plan. Client notification within 72 hours of confirmed breach involving their data.
Vulnerability Management	Regular dependency scanning and patching. No software installed in client environments. No VPN tunnels. No direct database access. All integrations are customer-authorized, outbound API connections from SiQ infrastructure.

Human-in-the-Loop (HITL) Governance

SiQ Cortex uses AI agents to analyze signals, score pipeline, and generate recommendations. In Assessment Mode, all output is delivered as a read-only report — no actions are taken in client systems. In Platform Mode, any external-facing action (outbound communications, CRM write operations, stakeholder alerts) requires explicit human approval through the HITL Approval Queue before execution.

HITL governance is a core architectural pattern, not an optional feature. It applies to every AI-generated recommendation that would result in a write action or external communication, including our AI SDR agent (Gage). No automated action fires without a human reviewing and approving it.

Compliance & Privacy

Framework	Status
SOC 2 Type II	Controls aligned; formal audit in progress.
CCPA	Compliant. No sale of personal information. Deletion requests honored within 14 business days.
GDPR	Not currently processing EU personal data. Framework in place for future EU expansion.
Data Processing Agreement	Available on request. Standard DPA covering processing scope, sub-processors, and deletion obligations.

Sub-Processors

Provider	Purpose	Data Exposure
Amazon Web Services	Cloud infrastructure, compute, storage	All client data (encrypted at rest and in transit)
Anthropic (Claude)	AI analysis, signal scoring, recommendation generation	Client CRM/pipeline data passed via API for analysis. Anthropic's commercial API terms prohibit use of customer inputs/outputs for model training. Data is not persisted by Anthropic beyond the API request lifecycle.
Airtable	Internal workflow coordination during assessment delivery	Assessment metadata and delivery status only (e.g., engagement name, milestone dates, deliverable status). No raw client CRM records, contact PII, or pipeline data stored in Airtable.

Questions & Contact

For security-related questions, additional documentation requests, or to schedule a call with our team, contact us at:

Email: info@scalientiq.com

Web: scalientiq.com

We're happy to jump on a call with your InfoSec team to walk through any of the above in detail.