Industrial Engineer AI — Integration Security Brief

Document Version: 1.0
Prepared by: Industrial Engineer AI
Contact: mike@industrialengineer.ai
Website: https://industrialengineer.ai/it-teams

Purpose

This document is prepared for IT Directors, Security Engineers, and InfoSec teams reviewing Industrial Engineer AI as a third-party integration vendor. It covers data access scope, authentication methods, data handling practices, infrastructure, and third-party dependencies.

1. Engagement Overview

Industrial Engineer AI is a specialist AI integration firm. We connect to your existing operational systems (WMS, ERP, TMS) via standard REST APIs to build live dashboards, automated reporting, and AI-powered analytics for your operations team.

We do not sell software licenses. We do not install agents on your servers. We do not require access to your network beyond standard HTTPS outbound to your existing API endpoints.

2. Data Access Scope

What We Access

- Operational transaction data from your WMS/ERP/TMS (order records, inventory counts, throughput metrics, shipment data)
- Only the specific endpoints required for the agreed-upon project scope
- Access scope is documented in writing before any production credentials are provisioned

What We Do NOT Access

- HR data, payroll records, or personally identifiable employee information
- Financial records beyond operational cost metrics (unless explicitly scoped)
- Customer PII beyond what is required for order tracking (and only with explicit approval)
- Any data outside the agreed project scope

Access Level

- **Default:** Read-only API access
- **Write access:** Only if explicitly required for a specific use case, scoped in writing, and approved by your IT team before implementation

---

3. Authentication & Credentials

Method	Details
OAuth 2.0	Preferred. We request a scoped token with minimum permissions.
API Key	Accepted. Keys are stored encrypted at rest, never logged.
Basic Auth	Accepted over HTTPS only.

Credential Storage:

- API credentials are stored in encrypted environment variables (AES-256)
- Credentials are never committed to source control
- Credentials are never logged in application logs
- Your team can revoke credentials at any time through your WMS admin panel

4. Data Handling & Retention

Practice	Our Policy
Data persistence	None by default. All queries run in real-time.
Caching	If required for performance: time-limited (5–15 min), scoped, disclosed in writing
Data transmission	TLS 1.2+ encryption in transit at all times
Data at rest	No operational data stored at rest on our servers
Data deletion	Upon project close, all credentials and any cached data are deleted
Audit trail	Full API call log available on request (endpoint, timestamp, parameters)

5. Infrastructure

Component	Details
Cloud provider	Amazon Web Services (AWS)
Primary region	us-east-1 (US East, N. Virginia)
Compute	AWS Lambda / ECS (serverless by default)
Network	No inbound access required to your network
Firewall requirements	Standard HTTPS outbound (port 443) to your API endpoints only

We do not require:

- VPN access to your network
- Firewall exceptions beyond standard HTTPS
- Installation of any software on your servers
- Access to your internal network

6. AI & Third-Party Dependencies

AI Inference

We use OpenAI and/or Anthropic APIs for natural language explanation of metrics (e.g., “Your pick rate dropped 12% on Tuesday — here’s why”).

Important: We do not send raw operational data to AI models. We send anonymized, aggregated metric summaries (e.g., “pick rate: 94.2 units/hr, down 12% vs. prior week”). No order numbers, customer names, or identifiable records are included in AI prompts.

Third-Party Services

Service	Purpose	Data Shared
OpenAI / Anthropic	Natural language metric explanation	Anonymized metric summaries only
AWS	Compute and infrastructure	Scoped operational data (encrypted)
Vercel / Cloudflare	Dashboard hosting and CDN	No operational data
Sentry (optional)	Error monitoring	Stack traces only, no operational data

7. Code & Intellectual Property

All integration code developed during the engagement is handed off to your team at project close. You receive:

- Full source code (TypeScript / Python)
- Architecture diagrams (system context, data flow)
- API documentation (endpoints accessed, parameters, response schemas)
- Runbooks (how to maintain, monitor, and troubleshoot the integration)

You own the code. We retain no rights to it after handoff. You are never dependent on Industrial Engineer AI to keep the integration running.

---

8. Compliance & Certifications

Item	Status
SOC 2 Type II	Not applicable (we are a specialist integration team, not a SaaS platform)
GDPR	We do not process EU personal data unless explicitly scoped
HIPAA	We do not process PHI unless explicitly scoped and a BAA is signed
Vendor security questionnaire	We will complete your questionnaire — contact us to request
Penetration testing	Available on request for enterprise engagements

---

9. Incident Response

In the event of a security incident:

1. We notify your IT team within 24 hours of discovery
2. We provide a written incident report within 72 hours
3. We revoke all credentials immediately upon discovery
4. We cooperate fully with your incident response process

Contact for security incidents: mike@industrialengineer.ai

---

10. Questions & Review Call

We are happy to answer any additional questions from your InfoSec team. We can schedule a 30-minute technical review call to walk through this document and answer questions in real time.

Book a call: https://calendly.com/mike-industrialengineer/industrial-engineer-ai-integration-solutions
IT Teams page: https://industrialengineer.ai/it-teams
Email: mike@industrialengineer.ai

Industrial Engineer AI — We work with your IT team, not around it.