NEXUS

NEXUS INDUSTRIAL GROUP, LLC
10601 Clarence Dr, Ste 250
Frisco, TX 75033 · USA
713.282.7440 · nexusindgroup.com

SECURITY RESPONSIBILITY SCHEDULE.

EXHIBIT B · MSA SCHEDULE

DOC NO.	VERSION	CLASSIFICATION
NXS-LEGAL-SEC	2.0 · 2026	Confidential

This Security Responsibility Schedule ("Security Schedule") is incorporated into the Master Services Agreement ("MSA") and the applicable Statement of Work ("SOW") between Nexus Industrial Group, LLC ("Nexus") and Client when referenced by the SOW. It allocates security responsibilities according to operational control.

01

SECTION

SECURITY PRINCIPLES

01 Client owns and controls production environments, production accounts, and production data unless an SOW expressly states otherwise.

02 Nexus implements agreed technical solutions and is responsible for Nexus-controlled access and systems.

03 Client determines the legal, regulatory, retention, business, and risk requirements applicable to Client and Client Data.

04 Security is a shared responsibility: each Party is responsible for controls within its possession or control.

05 Production credentials and privileged access should be minimized, time-bounded where practical, and removed promptly when no longer needed.

06 Managed security, monitoring, uptime, and 24/7 response obligations exist only if expressly included in a Managed Services SOW.

02

SECTION

ACCOUNT OWNERSHIP MATRIX

MOBILE PLATFORMS	Apple Developer / Google Play - Client owner; Client primary administrator; Nexus delegated access if required.
CLOUD INFRASTRUCTURE	AWS / Azure / Google Cloud / similar - Client owner; Client primary administrator; Nexus delegated access for implementation or support.
PAYMENT SYSTEMS	Stripe / PayPal / Authorize.net / similar - Client owner and administrator; Nexus implementation access only as needed.
AI PLATFORMS	OpenAI / Anthropic / Azure OpenAI / Gemini / similar - Client owner for production use unless the SOW expressly authorizes a Nexus-managed account.
COMMUNICATIONS	Twilio / SendGrid / Mailgun / Postmark / similar - Client owner for production use unless otherwise agreed.
IDENTITY / KYC	Persona / Veriff / SumSub / Onfido / similar - Client owner and administrator; Nexus delegated implementation access as needed.
ANALYTICS	Google Analytics / Mixpanel / Amplitude / similar - Client owner; Nexus access as needed for implementation or support.
SOURCE CONTROL / CI/CD	Client-owned repository for Client-owned production source code where practical; Nexus may use Nexus-controlled development repositories during active development subject to source-code delivery obligations.
SECRETS MANAGEMENT	Client-controlled production secrets store where practical; Nexus may hold only the minimum credentials reasonably necessary for Services.

03

SECTION

DEVELOPMENT AND TEST ENVIRONMENTS

Nexus may maintain development, sandbox, test, staging, source-control, and CI/CD environments for delivery of the Services. Temporary Nexus-controlled environments may be removed after project completion or transition. Client Data should not be

placed into a Nexus-controlled development environment unless reasonably necessary and approved or contemplated by the SOW.

04

SECTION

NEXUS ACCESS-CONTROL RESPONSIBILITIES

- Restrict access to authorized personnel with a business need.
- Use commercially reasonable authentication controls and require MFA for Nexus-controlled privileged accounts where supported.
- Apply least-privilege principles where practical.
- Remove or disable access for personnel promptly when no longer required.
- Use reasonable methods to protect credentials and avoid storing production secrets in source code or ordinary project documents.
- Notify Client when Nexus no longer needs delegated production access so access can be removed.

05

SECTION

CLIENT ACCESS-CONTROL RESPONSIBILITIES

- Manage production user, administrator, employee, and contractor access.
- Promptly revoke unauthorized, stale, or unnecessary access.
- Require MFA for privileged production accounts where the relevant platform supports it, unless Client knowingly elects otherwise.
- Protect Client credentials and prohibit unauthorized sharing.
- Maintain ownership and recovery methods for production accounts.

06

SECTION

DATA CLASSIFICATION AND SPECIAL HANDLING

Before Nexus receives or accesses data requiring special handling, Client will identify the data category and applicable requirements. Examples include personal information, biometric data, health information, financial information, payment-card data, export-controlled data, trade secrets, confidential customer data, and other regulated data.

Nexus is not responsible for undisclosed special handling requirements. If the project requires controls materially beyond Nexus's baseline safeguards, the Parties will document them in the SOW, a DPA, or another written security exhibit, together with any pricing or schedule impact.

07

SECTION

ENCRYPTION AND DATA TRANSFER

Nexus will use commercially reasonable encrypted transport for Client Confidential Information when supported by the applicable system. Encryption at rest, customer-managed keys, private networking, dedicated environments, or other enhanced controls are required only when identified in the SOW or applicable cloud architecture.

08

SECTION

BACKUPS, RETENTION, AND DISASTER RECOVERY

Unless an SOW expressly assigns an obligation to Nexus, Client is responsible for production backups, retention, disaster recovery, business continuity, restore testing, and archival requirements. Nexus may assist with design or implementation without assuming ongoing operational responsibility.

09

SECTION

SECURITY INCIDENT RESPONSE

9.1 NEXUS RESPONSIBILITIES

- After confirming a Security Incident affecting a Nexus-controlled system, notify Client without undue delay and, where commercially practicable, within seventy-two (72) hours after confirmation.
- Provide reasonably available information about the nature and scope of the incident.
- Take commercially reasonable steps to contain and remediate Nexus-controlled systems.
- Cooperate reasonably with Client in investigation and legally required response activities.

9.2 CLIENT RESPONSIBILITIES

- Manage notices to Client customers, employees, regulators, insurers, and the public unless law directly requires Nexus to notify.
- Manage legal, regulatory, business-continuity, and customer-support response for Client-controlled systems and data.
- Promptly provide Nexus relevant information regarding incidents originating in Client-controlled systems that may affect Nexus access or Services.

10

SECTION

THIRD-PARTY VENDOR SECURITY

Third-Party Services remain responsible for their own platforms, availability, and security. Nexus is not responsible for vendor breaches, outages, policy changes, API changes, pricing changes, or service discontinuation except to the extent directly

caused by Nexus's breach of its obligations in selecting, configuring, or using the vendor under the SOW.

11

SECTION

AI AND DATA HANDLING

- Client will identify whether production AI use may include personal, confidential, regulated, or proprietary data.
- Nexus will not knowingly use Client Confidential Information or Client Data to train a generalized Nexus model or generalized third-party model for unrelated customers without written authorization.
- Where commercially available and relevant, Nexus will use account settings or enterprise configurations intended to limit provider training or retention as identified in the SOW.
- Client is responsible for approving the categories of data that may be submitted to production AI providers.

12

SECTION

LOGGING, MONITORING, AND VULNERABILITY MANAGEMENT

Unless expressly included in a Managed Services SOW, Client is responsible for ongoing production monitoring, security-alert review, threat response, patch cadence for Client-controlled infrastructure, vulnerability management, and security operations. Nexus may provide implementation assistance but is not a managed security provider by default.

13

SECTION

PRODUCTION SUPPORT AND SERVICE LEVELS

Nexus has no obligation to provide 24/7 support, production monitoring, uptime guarantees, emergency response, or security operations unless expressly included in a Managed Services SOW or support addendum. Any SLA should define coverage hours, severity levels, response targets, exclusions, maintenance windows, dependencies, and service credits, if any.

14

SECTION

COMPLIANCE AND AUDIT SUPPORT

Client determines its compliance obligations. Nexus will provide reasonable information about Nexus-controlled security practices relevant to the Services, subject to confidentiality and protection of Nexus and third-party confidential information. Formal audits, penetration tests, questionnaires requiring material effort, customer-specific certifications, or on-site assessments are subject to reasonable advance notice and may require a separate agreement, NDA, or fee.

15

SECTION

CYBER INSURANCE

Each Party is responsible for obtaining insurance it considers appropriate. Any project-specific cyber-insurance requirement or minimum limit must be agreed in the SOW before project commencement.

16

SECTION

NO ABSOLUTE SECURITY GUARANTEE

Nexus will use commercially reasonable safeguards within the scope of this Schedule but does not guarantee absolute security or protection from all zero-day vulnerabilities, nation-state attacks, insider threats, credential theft, Internet failures, or vendor failures. Security obligations are limited to those expressly stated in the MSA, SOW, and this Schedule.

17

SECTION

SURVIVAL

Sections relating to confidentiality, data handling, incident cooperation, Client Data, and allocation of responsibility survive termination to the extent necessary to enforce accrued rights and obligations.