CYBERSECURITY RISK ASSESSMENT SERVICE AGREEMENT

PARTIES

This Cybersecurity Risk Assessment Service Agreement ("Agreement") is entered into as of January 22, 2024 ("Effective Date") by and between:

NEXUS INTELLIGENT SYSTEMS, INC., a Delaware corporation with principal offices at 1200 Technology Park Drive, San Jose, California 95134 ("Client")

AND

[CYBERSECURITY VENDOR NAME], a [STATE] corporation with principal offices at [FULL ADDRESS] ("Service Provider")

RECITALS

WHEREAS, Client operates a sophisticated enterprise AI services platform requiring comprehensive cybersecurity risk assessment;

WHEREAS, Service Provider specializes in advanced cybersecurity risk evaluation and mitigation strategies;

WHEREAS, the parties desire to establish a professional engagement for comprehensive cybersecurity risk assessment services;

NOW, THEREFORE, in consideration of the mutual covenants and agreements hereinafter set forth, the parties agree as follows:

1. DEFINITIONS

1 "Confidential Information" shall mean all proprietary technical, business, and operational information disclosed during the engagement, including but not limited to network architectures, system configurations, vulnerability reports, and strategic technology roadmaps.

2 "Risk Assessment" means a systematic evaluation of potential cybersecurity vulnerabilities, threat vectors, and potential operational risks within Client's technological infrastructure.

3 "Deliverables" shall include comprehensive written reports, vulnerability analysis documentation,

remediation recommendations, and executive summary presentations.

2. SCOPE OF SERVICES

1 Risk Assessment Methodology

Service Provider shall conduct a comprehensive cybersecurity risk assessment utilizing internationally recognized frameworks, including but not limited to:

- NIST Cybersecurity Framework
- ISO/IEC 27001 Standards
- CIS Critical Security Controls

2 Assessment Components

The risk assessment shall encompass:

a) Network infrastructure analysis

b) Application security evaluation

c) Cloud environment vulnerability scanning

d) Endpoint security assessment

e) Threat modeling and predictive risk analysis

3 Specific Evaluation Parameters

Service Provider will specifically assess:

- External and internal network penetration potential
- Authentication and access control mechanisms
- Data encryption protocols
- Incident response capabilities
- Third-party vendor security integrations

3. DELIVERABLES AND REPORTING

1 Comprehensive Report

Service Provider shall deliver:

- Detailed technical vulnerability report
- Executive summary with strategic recommendations
- Quantitative risk scoring methodology

- Prioritized remediation roadmap

2 Reporting Timeline

- Initial assessment report: Within 30 calendar days of engagement commencement
- Follow-up validation report: 90 days post-initial assessment

4. COMPENSATION

1 Fee Structure

Total engagement fee: $85,000, payable as follows:

- 30% upon contract execution
- 40% upon initial report delivery
- 30% upon completion of remediation consultation

2 Payment Terms

All invoices net 30 days, with late payments subject to 1.5% monthly interest charge.

5. CONFIDENTIALITY

1 Mutual Non-Disclosure

Both parties agree to maintain strict confidentiality regarding all shared information, implementing industry-standard protection protocols.

2 Data Protection

Service Provider shall:

- Implement AES-256 encryption for all transmitted data
- Utilize secure, access-controlled communication channels
- Permanently delete assessment data post-engagement

6. LIABILITY AND INDEMNIFICATION

1 Limitation of Liability

Total aggregate liability shall not exceed the total contract value of $85,000.

2 Professional Errors

Service Provider warrants professional performance consistent with industry best practices, providing

remediation for demonstrable errors of professional judgment.

7. TERMINATION

1 Termination Rights

Either party may terminate with 30 days written notice, with pro-rated compensation for services rendered.

8. GOVERNING LAW

This Agreement shall be governed by California law, with exclusive jurisdiction in Santa Clara County Superior Court.

9. SIGNATURES

IN WITNESS WHEREOF, the parties execute this Agreement as of the Effective Date.

NEXUS INTELLIGENT SYSTEMS, INC.

By:

Dr. Elena Rodriguez

Chief Executive Officer

Date: January 22, 2024

[CYBERSECURITY VENDOR]

By:

[Authorized Representative]

Title:

Date: