Enterprise Cybersecurity Framework Contract

PARTIES

This Enterprise Cybersecurity Framework Contract ("Agreement") is entered into as of January 22, 2024, by and between:

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

and

SECURE HORIZON TECHNOLOGIES, LLC, a California limited liability company with principal offices at 500 Technology Boulevard, Palo Alto, California 94304 ("Provider")

RECITALS

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

WHEREAS, Provider specializes in advanced cybersecurity framework design and implementation for technology-driven enterprises;

WHEREAS, the parties desire to establish a comprehensive cybersecurity framework to protect Client's intellectual property, customer data, and technological assets;

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

1. DEFINITIONS

1 "Cybersecurity Framework" shall mean the comprehensive set of technological, procedural, and administrative protocols designed to protect Client's digital infrastructure.

2 "Sensitive Data" shall include all proprietary algorithms, customer information, financial records, and strategic documentation generated or maintained by Client.

3 "Breach" shall mean any unauthorized access, exfiltration, or compromise of Client's digital systems or Sensitive Data.

2. SCOPE OF SERVICES

1 Framework Design

Provider shall develop a customized enterprise-grade cybersecurity framework tailored specifically to Client's technological ecosystem, including:

a) Comprehensive threat assessment

b) Multi-layered security architecture

c) Advanced intrusion detection mechanisms

d) Data encryption protocols

e) Incident response strategies

2 Implementation Phases

The cybersecurity framework shall be implemented in three distinct phases:

Phase I: Assessment and Planning (60 days)

Phase II: Infrastructure Deployment (90 days)

Phase III: Continuous Monitoring and Optimization (Ongoing)

3. SECURITY REQUIREMENTS

1 Minimum Security Standards

Provider guarantees the following minimum security standards:

a) 256-bit AES encryption for all data transmissions

b) Multi-factor authentication protocols

c) Real-time threat monitoring

d) Quarterly comprehensive security audits

e) Immediate breach notification within 4 hours of detection

2 Compliance Frameworks

The cybersecurity framework shall be compliant with:

- NIST Special Publication 800-53
- ISO/IEC 27001:2022
- SOC 2 Type II Standards

- GDPR Data Protection Requirements

4. FINANCIAL TERMS

1 Compensation Structure

Client shall compensate Provider as follows:

a) Initial Framework Design: $175,000

b) Implementation Services: $250,000

c) Annual Maintenance and Optimization: $125,000 per year

2 Payment Schedule

- 30% upon contract execution
- 40% upon completion of Phase II
- 30% upon successful framework validation

5. LIABILITY AND INDEMNIFICATION

1 Limitation of Liability

Provider's total aggregate liability shall not exceed the total contract value of $550,000, excluding cases of gross negligence or willful misconduct.

2 Indemnification

Provider shall indemnify Client against direct damages resulting from:

a) Negligent framework design

b) Failure to implement agreed-upon security protocols

c) Breach of contractual security obligations

6. TERM AND TERMINATION

1 Initial Term

This Agreement shall commence on the effective date and continue for an initial period of twenty-four (24) months.

2 Renewal

The Agreement may be renewed for successive twelve-month periods upon mutual written consent.

3 Termination Conditions

Either party may terminate the Agreement with sixty (60) days written notice in the event of a material breach.

7. CONFIDENTIALITY

1 Confidential Information

Both parties agree to maintain strict confidentiality regarding all shared technical, strategic, and operational information.

2 Non-Disclosure

Unauthorized disclosure shall result in immediate contract termination and potential legal action.

8. GOVERNING LAW

This Agreement shall be governed by and construed in accordance with the laws of the State of California.

9. SIGNATURES

IN WITNESS WHEREOF, the parties have executed this Enterprise Cybersecurity Framework Contract as of the date first above written.

NEXUS INTELLIGENT SYSTEMS, INC.

By:

Dr. Elena Rodriguez

Chief Executive Officer

SECURE HORIZON TECHNOLOGIES, LLC

By:

Jonathan Reyes

Chief Executive Officer