Cybersecurity Consulting Engagement - Risk Management Protocol

PARTIES

This Cybersecurity Risk Management Protocol ("Protocol") is entered into as of January 22, 2024, by and between:

Nexus Intelligent Systems, Inc., a Delaware corporation with principal offices at 1200 Technology Park Drive, San Jose, California 95134 ("Client")

and

CyberShield Solutions, LLC, a cybersecurity consulting firm with principal offices at 500 Innovation Way, Austin, Texas 78758 ("Consultant")

RECITALS

WHEREAS, Client operates a sophisticated enterprise AI services platform with complex digital infrastructure requiring advanced cybersecurity risk management;

WHEREAS, Consultant possesses specialized expertise in enterprise-level cybersecurity risk assessment and mitigation strategies;

WHEREAS, the parties desire to establish a comprehensive protocol for identifying, evaluating, and managing cybersecurity risks;

1. ENGAGEMENT SCOPE

1 Comprehensive Risk Assessment

Consultant shall conduct a comprehensive cybersecurity risk assessment encompassing:

a) Network infrastructure vulnerability analysis

b) Application security evaluation

c) Data protection protocol review

d) Threat landscape mapping

e) Compliance framework validation

2 Deliverables

The engagement will produce:

- Detailed risk assessment report
- Prioritized remediation recommendations
- Executive summary briefing
- Technical implementation roadmap

2. RISK MANAGEMENT METHODOLOGY

1 Assessment Framework

Consultant shall utilize the following standardized methodological approach:

- NIST Special Publication 800-53 security controls
- ISO/IEC 27001 information security standards
- MITRE ATT&CK framework threat modeling

2 Analytical Dimensions

Risk evaluation will encompass:

a) Technical vulnerability assessment

b) Operational security gaps

c) Potential financial and reputational impact

d) Regulatory compliance risks

3. CONFIDENTIALITY PROVISIONS

1 Proprietary Information

Both parties acknowledge potential exposure to confidential information and agree to:

- Implement strict non-disclosure protocols
- Protect all shared technical documentation
- Restrict information access to authorized personnel
- Maintain comprehensive audit trails of information handling

2 Data Protection

Consultant shall:

- Encrypt all transmitted and stored client information
- Utilize secure communication channels

- Implement multi-factor authentication for data access
- Comply with GDPR and CCPA data protection standards

4. ENGAGEMENT PARAMETERS

1 Duration

- Initial assessment period: 45 calendar days
- Comprehensive report delivery: Within 60 days of contract execution
- Optional follow-up consultation: 90-day post-report support window

2 Financial Terms

- Total engagement value: $175,000
- Payment schedule:
- 30% upon contract execution
- 40% upon interim report delivery
- 30% upon final report acceptance

5. LIABILITY AND INDEMNIFICATION

1 Limitation of Liability

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

2 Indemnification

Each party shall indemnify the other against third-party claims arising from material breach of contractual obligations.

6. TERMINATION PROVISIONS

1 Termination Rights

Either party may terminate the engagement with 30 days written notice if material breach occurs.

2 Post-Termination Obligations

Upon termination, Consultant shall:

- Provide all completed work products
- Destroy or return confidential materials

- Cease all active information gathering

7. GOVERNING LAW

This Protocol shall be governed by the laws of the State of California, with exclusive jurisdiction in Santa Clara County.

SIGNATURES

\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

Dr. Elena Rodriguez, CEO

Nexus Intelligent Systems, Inc.

\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

Michael Thompson, Managing Partner

CyberShield Solutions, LLC

Date: January 22, 2024