

CYBERSECURITY ASSESSMENT AND REMEDIATION CONTRACT

PARTIES

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

SecureCore Technologies, LLC ("Service Provider"), a Delaware limited liability company with principal offices at 1200 Technology Park Drive, Austin, Texas 78758

AND

Nexus Intelligent Systems, Inc. ("Client"), a Delaware corporation with principal offices at 550 Market Street, Suite 400, San Francisco, California 94105

RECITALS

WHEREAS, Nexus Intelligent Systems, Inc. operates a complex enterprise AI platform requiring comprehensive cybersecurity assessment and strategic remediation;

WHEREAS, SecureCore Technologies possesses specialized expertise in advanced cybersecurity diagnostics and enterprise risk mitigation;

WHEREAS, the parties desire to establish a comprehensive framework for identifying, evaluating, and resolving potential cybersecurity vulnerabilities;

NOW, THEREFORE, the parties agree as follows:

1. DEFINITIONS

1 "Assessment" shall mean the comprehensive cybersecurity evaluation conducted by Service Provider, including but not limited to:

- a) Network infrastructure analysis
- b) Application security testing
- c) Vulnerability scanning
- d) Penetration testing protocols
- e) Threat landscape evaluation

2 "Remediation Plan" shall mean the detailed strategic document outlining specific actions, timelines, and recommended interventions to address identified security vulnerabilities.

3 "Confidential Information" shall include all technical, operational, and strategic data exchanged during the assessment process.

2. SCOPE OF SERVICES

1 Assessment Methodology

Service Provider shall conduct a comprehensive, multi-phase cybersecurity assessment utilizing industry-standard methodologies, including:

- a) Initial reconnaissance and information gathering
- b) Vulnerability identification
- c) Risk prioritization
- d) Detailed reporting

2 Specific Assessment Components

The assessment shall encompass:

- a) External network perimeter analysis
- b) Internal network infrastructure evaluation
- c) Cloud infrastructure security review
- d) Application and API security testing
- e) Identity and access management assessment
- f) Data protection and encryption protocols review

3. DELIVERABLES

1 Service Provider shall provide the following deliverables:

- a) Comprehensive Cybersecurity Assessment Report
- b) Detailed Remediation Roadmap
- c) Executive Summary Presentation
- d) Technical Findings Documentation

2 Reporting Specifications

- Detailed risk categorization (Critical, High, Medium, Low)

- Quantitative and qualitative risk analysis
- Recommended mitigation strategies
- Estimated implementation complexity and resource requirements

4. ENGAGEMENT TIMELINE

1 The total engagement duration shall be twelve (12) weeks, structured as follows:

- Week 1-2: Initial assessment and reconnaissance
- Week 3-6: Comprehensive vulnerability testing
- Week 7-9: Analysis and report preparation
- Week 10-12: Remediation planning and knowledge transfer

5. COMPENSATION

1 Total Contract Value: \$185,000, structured as:

- Initial Assessment: \$95,000
- Detailed Remediation Planning: \$60,000
- Follow-up Consultation: \$30,000

2 Payment Schedule

- 30% upon contract execution
- 40% upon completion of initial assessment
- 30% upon delivery of final remediation roadmap

6. CONFIDENTIALITY

1 Both parties agree to maintain strict confidentiality regarding all shared information, with obligations continuing for three (3) years post-engagement.

2 All assessment findings shall be considered proprietary and confidential, with limited disclosure authorized only to Client's designated executive leadership.

7. LIABILITY AND INDEMNIFICATION

1 Service Provider's total liability shall not exceed the total contract value.

2 Client agrees to provide complete, accurate system access and information necessary for

comprehensive assessment.

8. GOVERNING LAW

This Agreement shall be governed by the laws of the State of California, with any disputes subject to arbitration in San Francisco County.

9. SIGNATURES

IN WITNESS WHEREOF, the parties have executed this Agreement as of the date first above written.

SecureCore Technologies, LLC

By:

Name: Dr. Marcus Reyes

Title: Chief Executive Officer

Date: January 22, 2024

Nexus Intelligent Systems, Inc.

By:

Name: Dr. Elena Rodriguez

Title: Chief Executive Officer

Date: January 22, 2024