Cybersecurity Infrastructure Asset Register

Confidential Document

Nexus Intelligent Systems, Inc.

Proprietary and Confidential

Document Control

Document Version: 1.2

Effective Date: January 22, 2024

Classification: Internal Use - Restricted Access

1. Purpose and Scope

1 This Cybersecurity Infrastructure Asset Register ("Register") serves as the comprehensive inventory and documentation of all critical technology infrastructure, network assets, and digital systems maintained by Nexus Intelligent Systems, Inc. (hereinafter "Company").

2 The purpose of this Register is to:

a) Provide a definitive record of all technology assets

b) Support cybersecurity risk management

c) Enable comprehensive asset tracking and lifecycle management

d) Facilitate regulatory compliance and due diligence processes

2. Definitions

1 "Critical Asset" shall mean any technological infrastructure, hardware, software, or network component essential to the Company's operational continuity and data protection strategy.

2 "Asset Classification" refers to the systematic categorization of technological resources based on their strategic importance, potential risk exposure, and operational criticality.

3. Asset Inventory Methodology

1 Asset Identification Process

a) Comprehensive physical and virtual asset mapping

b) Quarterly validation and update protocols

c) Multi-factor verification of asset ownership and configuration

2 Classification Criteria

- Operational Criticality
- Data Sensitivity
- Replacement Cost
- Potential Security Risk Exposure

4. Infrastructure Asset Categories

4.1 Network Infrastructure

- Core Network Switches: 12 enterprise-grade Cisco Nexus 9000 series
- Firewall Systems: 4 clustered Palo Alto Networks PA-5200 series
- Load Balancers: 2 F5 BIG-IP 6900 appliances
- VPN Concentrators: 3 Fortinet FortiGate 3700D systems

4.2 Cloud Infrastructure

- Primary Cloud Provider: Amazon Web Services (AWS)
- Secondary Cloud Provider: Microsoft Azure
- Total Cloud Instances: 87 distributed compute nodes
- Cloud Storage: 672 TB distributed storage capacity

4.3 Endpoint Devices

- Total Employee Laptops: 79 (MacBook Pro and Dell Precision)
- Server Infrastructure: 22 on-premise rack-mounted servers
- Development Workstations: 16 high-performance compute nodes

5. Security Control Mapping

1 Each asset is mapped to specific security control frameworks:

- NIST SP 800-53
- ISO 27001
- SOC 2 Type II Compliance Standards

2 Security Control Categories:

a) Access Management

b) Encryption Protocols

c) Network Segmentation

d) Incident Response Capabilities

6. Maintenance and Update Protocols

1 This Register shall be:

- Reviewed quarterly
- Validated by Chief Technology Officer
- Updated within 5 business days of any material change

2 Mandatory Update Triggers:

- New asset acquisition
- Decommissioning of existing assets
- Significant configuration modifications

7. Confidentiality and Limitations

1 This document contains proprietary and confidential information. Unauthorized disclosure is strictly prohibited.

2 While comprehensive, this Register represents a point-in-time assessment and is subject to ongoing refinement.

8. Execution

Executed this 22nd day of January, 2024.

_

Michael Chen

Chief Technology Officer

Nexus Intelligent Systems, Inc.

9. Disclaimer

This document is provided for informational purposes and does not constitute a comprehensive security assessment. Professional consultation is recommended for specific implementation strategies.